IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

JEFFREY WARREN DIXON, HOLLIE MOORE, STEVEN B. STEIN, JOHN CORONA, ANNA RICE-WRIGHT, JAMES R. WRIGHT, CHRISTOPHER P. DUNLEAVY, VICTORIA LYNN STRUTZ, PHILLIP WILLIAMS, JON M. LEWIS, STEPHEN M. SHAFRAN, JR., BARBARA A. SHAFRAN, GARY MARTINEZ, JULIA A. WILLIAMS, KATHERINE EDWARDS, JOHN L. BRISINI, JR., RYAN TREAT, ANTONIETTA MCCANN, PATRICIA SAMUELSON, DONALD A. CORDELL, DEBORAH RIVAS, RANDALL K. ROSHTO, ELIZABETH DORSSOM, and KAREN BERGQUIST individually and on behalf of all others similarly situated,

Plaintiffs,

v.

EQUIFAX, INC.,

Defendant.

CIVIL ACTION

TABLE OF CONTENTS

I. **INTRODUCTION** 1

II. PARTIES 3

A. Plaintiffs 3

B. Defendant 7

III. JURISDICTION AND VENUE 8

IV. FACTUAL ALLEGATIONS 9

A. Equifax Was Negligent in Its Efforts to Protect Highly Valuable Personal Information 9

B. Equifax Failed to Release News of the Massive Breach Within a Timely Manner, and Its Response Has Been Deeply Flawed 13

C. Equifax's Failures Have Harmed and Will Continue to Harm Breach Victims 18

V. CLASS ACTION ALLEGATIONS 22

A. Class Definition(s) 22

1. National Class 22

2. Statewide Classes 22

VI. CLAIMS FOR RELIEF 26

COUNT I — Willful Violation of The Fair Credit Reporting Act, 15 U.S.C. §§ 1681 et seq. 26

1. Overview 26

2. Violations of 15 U.S.C. § 1681e(a) – Willful Failure to Maintain Reasonable Security Measures 28

3. Violations of 15 U.S.C. § 1681b(a) – Furnishing Consumer Data Without a Permissible Purpose.....................30

4. Violations of 15 U.S.C. § 1681b(g) – Willful Disclosure of Confidential Medical Data 31

5. Violations of 15 U.S.C. § 1681c-1 – Willful Failure to Respond to Suspected Identify Theft 32

6. Plaintiffs and the Nationwide Class Suffered Damages as a Proximate Result of Equifax's Willful Violations of FCRA and are Entitled to Relief..33

COUNT II — Negligent Violation of the Fair Credit Reporting Act 36

COUNT III — Negligence 41

COUNT IV — Negligence Per Se...45

COUNT V — Declaratory Judgment..52

7. Claims Asserted on Behalf of Statewide Classes 55

COUNT VI — Violation of the Georgia Uniform Deceptive Trade Practices Act, O.C.G.A. §§ 10-1-370 et seq. 55

COUNT VII — Violation of the Georgia Security Breach Notification Act, O.C.G.A. §§ 10-1-912 et seq. 59

COUNT VIII — Violation of the California Customer Records Act California Civil Code Section 1798.80 et seq. 61

COUNT IX — Violation of California's Unfair Competition Law, California Business and Professions Code Section 17200 et seq. 66

COUNT X — Violation of Virginia Personal Information Breach Notification Act, Va. Code. §§ 18.2-186.6 et seq................72

COUNT XI — Violation of Virginia Code Annotated § 18.2-186.6 73

COUNT XII — Violation of The New Jersey Consumer Fraud Act N.J. Stat. Ann. §§ 56:8-1 et seq..76

COUNT XIII — Violation of the New Jersey Customer Security Breach Disclosure Act N.J. Stat. Ann. §§ 56:8-163 et seq..78

COUNT XIV — Violation of the Washington Data Brach Notice Act, Wash. Rev. Code. §§ 19.255.10 et seq. 80

COUNT XV — Violation of Washington Consumer Protection Act, Wash. Rev. Code §§ 19.86.020 et seq......................................82

COUNT XVI — Violation of The District of Columbia Consumer Protection Procedures Act, D.C. Code §§ 28-3904 et seq...85

COUNT XVII — Violation of the District of Columbia Consumer Security Breach Notification Act, D.C. Code § 28-3851, et. seq. 87

COUNT XVIII — Violations of Pennsylvania Unfair Trade Practices And Consumer Protection Law, 73 Pa. Stat. §§ 201-1 et seq. 89

COUNT XIX — Violation of the Delaware Consumer Fraud Act, 6 Del. Code §§ 2513 et seq..92

COUNT XX — Violation of the Delaware Computer Security Breach Act, 6 Del. Code §§ 12B-102 et seq. 95

COUNT XXI — Violation of Florida's Unfair & Deceptive Trade Practices Act, Fla. Stat. §§ 501.201 et seq..............................97

COUNT XXII — Violation of South Carolina Data Breach Security Act, S.C. Code Ann. §§ 39-1-90 et seq. 100

COUNT XXIII — Violations of South Carolina Unfair Trade Practices Act, S.C. Code Ann. §§ 39-5-10 et seq. 102

COUNT XXIV — Violation of the Louisiana Security Breach Disclosure Act, La. Rev. Stat. §§ 51:3074 et seq............................105

COUNT XXV — Violation of the Missouri Merchandise Practicing Act, Mo. Stat. §§ 407.010 et seq...................................106

COUNT XXVI — Violations of Alabama's Deceptive Trade Practices Act, Code of Ala. §§ 8-19-1 et seq. 109

VII. PRAYER FOR RELIEF 113

VIII. DEMAND FOR JURY TRIAL 114

PLAINTIFFS' CLASS ACTION COMPLAINT

Plaintiffs bring this action on behalf of themselves and all others similarly situated, against Equifax, Inc. ("Defendant"). Plaintiffs allege the following based upon information and belief, the investigation of counsel, and personal knowledge as to the factual allegations pertaining to himself/herself.

I. INTRODUCTION

1. Equifax, one of the nation's three large credit reporting agencies, trades in the personal information of tens of millions of Americans. Those who trust that information to Equifax have a right to expect that it uses the best possible information security infrastructure and practices. Unfortunately for nearly half of the nation's population, that appears not to have been the case.

2. On September 7th, Equifax disclosed that it had experienced a data breach that has exposed the most sensitive identifying information of 143 million Americans (the "Data Breach"). That includes names, dates of birth, and Social Security numbers: the essential raw materials for identity thieves. The breach also exposed phone numbers, credit card numbers, and driver's license numbers.

3. The Data Breach does not appear to have been technically sophisticated. Rather, hackers were able to gain access through a common web application with a known vulnerability that reportedly was not properly secured.

4. Once the hackers had access, they had months to search for and obtain the most valuable information for identity thieves before Equifax discovered the breach. Although Equifax knew about the breach for months, it did not tell the tens of millions of victims of that breach until September 7th. And Equifax's response since then has been, to put it charitably, bumbling.

5. Since its initial disclosure on September 7, Equifax subsequently confirmed that it experienced a separate major breach of it systems in March which appear to involve the same intruders. Equifax's Chairman and CEO Richard F. Smith announced his retirement following the Data Breach.

6. As a result of Equifax's negligence, tens of millions of Americans are now at increased risk of financial account fraud, tax fraud, and other forms identity theft. That increased risk will last for years, because the non-changeable identifying information has absolutely no shelf life.

7. To redress that and other harms caused by what is already being called the worst consumer data breach in history, Plaintiffs brings this action on behalf of themselves and a proposed nationwide class of similarly situated victims, seeking all available remedies.

II. PARTIES

A. Plaintiffs

1. Class representative Jeffrey Warren Dixon is a U.S. Citizen and resident of Tift County, Georgia. Mr. Dixon's data was compromised, damaged, and otherwise put at risk by Equifax's gross negligence and other violations of law.

2. Class representative Hollie Moore is a U.S. Citizen and resident of Troup County, Georgia. Ms. Moore's data was compromised, damaged, and otherwise put at risk by Equifax's gross negligence and other violations of law.

3. Class representative Steven B. Stein is a U.S. Citizen and resident of Marin County, California. Mr. Stein's data was compromised, damaged, and otherwise put at risk by Equifax's gross negligence and other violations of law.

4. Class representative John Corona is a U.S. Citizen and resident of Contra Costa, California. Mr. Corona's data was compromised, damaged, and otherwise put at risk by Equifax's gross negligence and other violations of law.

5. Class representatives Anna Rice-Wright and James R. Wright are U.S. Citizens and resident of Hanover County, Virginia. Ms. Rice-Wright's and Mr. Wright's data was compromised, damaged, and otherwise put at risk by Equifax's gross negligence and other violations of law.

6. Class representative Christopher P. Dunleavy is a U.S. Citizen and resident of Bergen County, New Jersey. Mr. Dunleavy's data was compromised, damaged, and otherwise put at risk by Equifax's gross negligence and other violations of law. Mr. Dunleavy enrolled in Equifax's identity protection and credit monitoring "Premier Plan" in 2011 and upgraded to the "Complete Family Plan" in 2014 at additional cost.

7. Class representative Victoria Lynn Strutz is a U.S. Citizen and resident of Thurston County, Washington. Ms. Strutz's data was compromised, damaged, and otherwise put at risk by Equifax's gross negligence and other violations of law.

8. Class representative Deborah Rivas is a U.S. Citizen and resident of Snohomish County, Washington. Ms. Rivas's data was compromised, damaged, and otherwise put at risk by Equifax's gross negligence and other violations of law.

9. Class representative Phillip Williams is a U.S. Citizen and resident of Washington, D.C. Mr. Williams's data was compromised, damaged, and otherwise put at risk by Equifax's gross negligence and other violations of law.

10. Class representative Jon M. Lewis is a U.S. Citizen and resident of Westmoreland County, Pennsylvania. Mr. Lewis's data was compromised,

damaged, and otherwise put at risk by Equifax's gross negligence and other violations of law.

11. Class representatives Stephen M. Shafran, Jr. and Barbara A. Shafran are U.S. Citizens and residents of Westmoreland County, Pennsylvania. Mr. and Ms. Shafran's data was compromised, damaged, and otherwise put at risk by Equifax's gross negligence and other violations of law.

12. Class representative Gary Martinez is a U.S. Citizen and resident of New Castle County, Wilmington, Delaware. Mr. Martinez's data was compromised, damaged, and otherwise put at risk by Equifax's gross negligence and other violations of law.

13. Class representative Julia A. Williams is a U.S. Citizen and resident of Palatka, Florida. Ms. Williams' data was compromised, damaged, and otherwise put at risk by Equifax's gross negligence and other violations of law.

14. Class representative Katherine Edwards is a U.S. Citizen and resident of Manatee County, Florida. Ms. Edwards data was compromised, damaged, and otherwise put at risk by Equifax's gross negligence and other violations of law.

15. Class representative John L. Brisini, Jr. is a U.S. Citizen and resident of Charleston County, South Carolina. Mr. Brisini's data was compromised,

damaged, and otherwise put at risk by Equifax's gross negligence and other violations of law.

16. Class representative Ryan Treat is a U.S. Citizen and resident of Charleston County, South Carolina. Mr. Treats's data was compromised, damaged, and otherwise put at risk by Equifax's gross negligence and other violations of law.

17. Class representative Antonietta McCann is a U.S. Citizen and resident of Charleston, South Carolina. Ms. McCann's data was compromised, damaged, and otherwise put at risk by Equifax's gross negligence and other violations of law.

18. Class representative Donald A. Cordell is a U.S. Citizen and resident of Charleston County, South Carolina. Mr. Cordell's data was compromised, damaged, and otherwise put at risk by Equifax's gross negligence and other violations of law.

19. Class representative Patricia Samuelson is a U.S. Citizens and resident of Dorchester County, South Carolina. Ms. Samuelson's data was compromised, damaged, and otherwise put at risk by Equifax's gross negligence and other violations of law.

20. Class representative Randall K. Roshto is a U.S. Citizen and resident of East Baton Rouge, Baton Rouge, Louisiana. Mr. Roshto's data was

compromised, damaged, and otherwise put at risk by Equifax's gross negligence and other violations of law.

21. Class representative Elizabeth Dorssom is a U.S. Citizen and resident of Boone County, Missouri. Ms. Dorssom's data was compromised, damaged, and otherwise put at risk by Equifax's gross negligence and other violations of law.

22. Class representative Karen Bergquist is a U.S. Citizen and resident of Jefferson County, Alabama. Ms. Bergquist's data was compromised, damaged, and otherwise put at risk by Equifax's gross negligence and other violations of law.

B. Defendant

23. Equifax Inc. is a global company headquartered in Atlanta, Georgia that does business throughout the country and is one of the three primary credit reporting agencies in the United States. Equifax maintains data on more than 820 million consumers worldwide. The company employs approximately 9,900 people and operates or has investments in 24 countries in North America, Central and South America, Europe and the Asia Pacific region. Among Equifax's subsidiaries is Equifax Information Services, LLC, which collects and reports consumer information to financial institutions

III. JURISDICTION AND VENUE

24. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 based on the federal statutory claims below, and the Court has supplemental jurisdiction over Plaintiffs' state law claims under 28 U.S.C. § 1367.

25. This Court also has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because at least one Class member is of diverse citizenship from one defendant, there are 100 or more Class members nationwide, and the aggregate amount in controversy exceeds $5,000,000.

26. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(3) because the Court has personal jurisdiction over Defendant, a substantial portion of the alleged wrongdoing occurred in this District and Georgia, and Defendant has sufficient contacts with this District and Georgia.

27. Venue is proper in the Northern District of Georgia pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claims at issue in this Complaint arose in this District.

IV. FACTUAL ALLEGATIONS

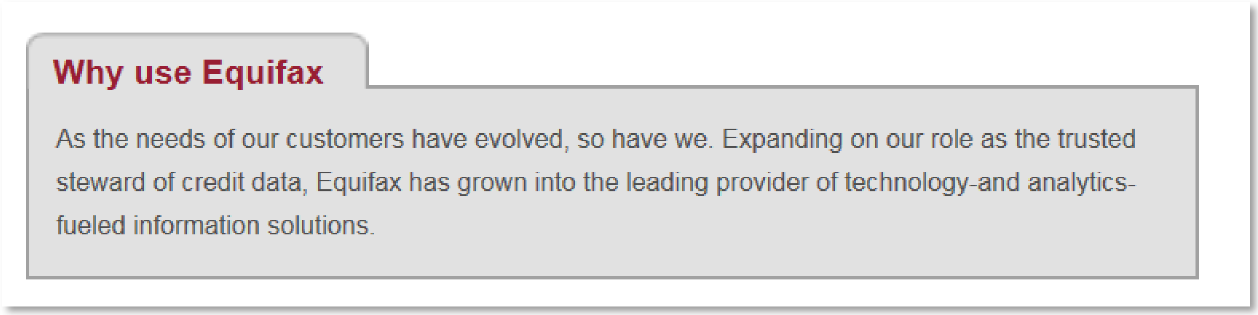
A. Equifax Was Negligent in Its Efforts to Protect Highly Valuable Personal Information

28. Equifax is one of the largest credit reporting agencies in the world. It profits by reporting on people's most sensitive financial information, and touts its "commitment to . . . protect the privacy and confidentiality of personal information about consumers." But hackers gained access to the personal information Equifax pledged to protect, not as a result of a complex attack, but, rather, they exploited a known flaw in a common open-source web development software.

29. The hackers, according to the company, "exploited a U.S. website application vulnerability to gain access to certain files." This vulnerability is a part of a software package for building web applications called Apache Struts. Apache reported the bug in March. Although Equifax was aware of the vulnerability, it reportedly failed to patch all of its systems with a security update, even though hackers were already taking advantage of that vulnerability elsewhere at that time. For more than four months, Equifax left open a known vulnerability that hackers could easily exploit to access the private data of almost half of all Americans. As a result, hackers "roamed undetected in Equifax Inc.'s computer network for more than four months before its security team uncovered the massive data breach[.]"

30. Equifax's failure to patch a known vulnerability is contrary to its public representations about its data security and in violation of its duty to protect the public's credit data.

31. Equifax has represented that it is a "trusted steward of credit data" and had sufficient information security to protect that data:


Why use Equifax

As the needs of our customers have evolved, so have we. Expanding on our role as the trusted steward of credit data, Equifax has grown into the leading provider of technology-and analytics-fueled information solutions.

32. In a 2011 report, "Leading With Integrity: The Equifax Business Ethics and Compliance Program," Equifax explained that the Gramm-Leach-Bliley Act required financial institutions to "develop and maintain an information security program to protect the security, confidentiality and integrity of the information." The report also represented that "Equifax entities that receive and collect consumer and customer information have developed and maintain appropriate information security programs."

33. Nonetheless, it appears Equifax did not have sufficient infrastructure or procedures to prevent the intrusion. It also appears that Equifax did not have sufficient infrastructure or procedures to detect the intrusion once it occurred. Once

the hackers were able to gain access, they appear to have had that access for months, which suggests Equifax had very poor security detection practices.

34. Equifax's negligence in failing to identify and deter the May intrusion is exacerbated in light of the Company's September 13th disclosure that it experienced another major breach just two months before, in March, which involved the same intruders. In response, Equifax hired security firm Mandiant to investigate the March breach and notified the incident to customers, affected individuals and regulators. The Company has stated that the hacks involved customer databases unrelated to those implicated in the breach discovered July 29.

35. Equifax's international data security practices suggest the company had a poor information security corporate culture. A group of security researchers in Argentina recently discovered that Equifax's employee portal to manage credit disputes from customers in that country "was wide open, protected by perhaps the most easy-to-guess password combination ever: 'admin/admin.'" Inside that portal, researchers could reportedly easily discover employee login and password information. Most troubling, the researchers could easily find customers' DNI, the Argentinian equivalent of a Social Security number. "To me, this is just negligence," one of the researchers told Brian Krebs. "In this case, their approach

to security was just abysmal, and it's hard to believe the rest of their operations are much better."

36. A former lead information analyst told reporters that Equifax shared unmasked social security numbers to company overseas. The employee said the company treated people's personally identifiable information as a "commodity."

37. Aa a result of the Data Breach and its aftermath, Equifax Chairman and CEO Richard F. Smith stepped down. Equifax also fired its chief information officer and chief security officer. The chief security officer, a college music major, had been criticized for lacking qualifications.

38. Congress and more than 30 states attorneys general are investigating the Data Breach. The Federal Trade Commission, in an unusual disclosure, said that it is also investigating the Data Breach.

39. Rather than spend adequate resources on data security, Equifax reportedly spent hundreds of thousands of dollars seeking to "reform" laws that impose liability on credit reporting agencies or require strict reporting of data breaches. In the months preceding the Data Breach, Equifax Inc. was lobbying lawmakers and federal agencies to ease up on regulation of credit-reporting companies. According to its congressional lobbying-disclosure reports, Equifax

spent at least $500,000 on lobbying Congress and federal regulators in the first half of 2017.

B. Equifax Failed to Release News of the Massive Breach Within a Timely Manner, and Its Response Has Been Deeply Flawed

40. Equifax reportedly discovered the Data Breach in July, but did not disclose the breach to the American public until September 7th. For months, consumers were unaware that some of their most valuable private information could be open, seen, and used by anybody. This personal information could include data about loans, loan payments and credit cards, as well as information on everything from child support payments, credit limits, missed rent and utilities payments, addresses and employer history, which all factor into credit scores.

41. The impact of Equifax's delayed disclosure has been compounded by a botched response rollout, causing affected individuals additional harm and frustration. As computer security expert Brian Krebs wrote, "I cannot recall a previous data breach in which the breached company's public outreach and response has been so haphazard and ill-conceived as the one coming right now from big-three credit bureau Equifax."

42. To begin with, the website that Equifax created to belatedly notify people of the Data Breach, www.equifaxsecurity2017.com, wrote Krebs, is "completely broken at best, and little more than a stalling tactic or sham at worst."

For example, the website operates on a stock installation WordPress, which does not provide adequate security for website on which Equifax asks data breach victims to provide their last names and most of the Social Security number. As another indication of Equifax's slipshod approach, as reported by Ars Technica, Equifax left a username for administering the site in a page hosted on that site, "something that should never have happened":

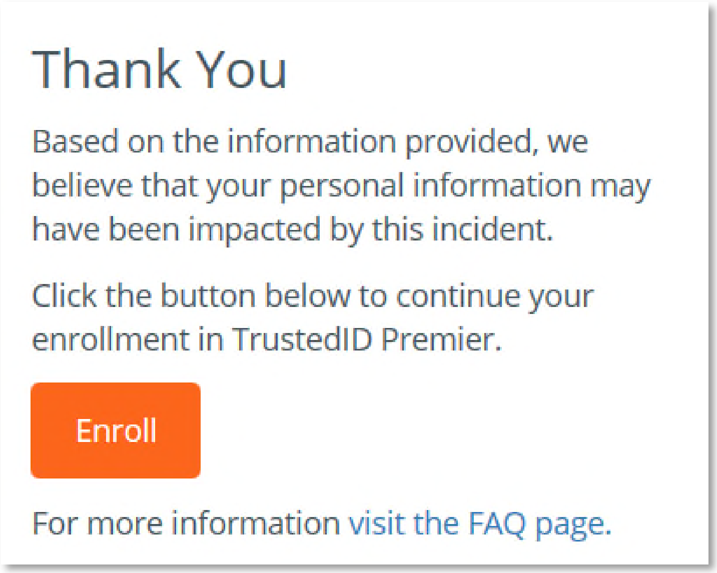
Secure | https://www.equifaxsecurity2017.com/wp-json/wp/v2/users/
[redacted]
[{"id":1,"name":"edelman","url":"","description":"","link":"https:\/\/www.equifaxsecurity2017.com\/author\/edelman\/","slug":"edelman","avatar_urls":{"24":"https:\/\/secure.gravatar.com\/avatar\/6f663bcf3fe53adc928a8eae7c7b66bc?s=24&d=mm&r=g","48":"https:\/\/secure.gravatar.com\/avatar\/6f663bcf3fe53adc928a8eae7c7b66bc?s=48&d=mm&r=g","96":"https:\/\/secure.gravatar.com\/avatar\/6f663bcf3fe53adc928a8eae7c7b66bc?s=96&d=mm&r=g"},"meta":[],"_links":{"self":[{"href":"https:\/\/www.equifaxsecurity2017.com\/wp-json\/wp\/v2\/users\/1"}],"collection":[{"href":"https:\/\/www.equifaxsecurity2017.com\/wp-json\/wp\/v2\/users"}]}}]

43. Those victims who were able to access the Equifax website to verify if they were victims of the Data Breach encountered more evidence of Equifax's bumbling response. To use the website, it appeared that Equifax was asking victims to give up any right to sue TrustedID, an Equifax entity providing identity monitoring services. Equifax appears to have changed the terms of service for that website after an outcry from consumers and consumer protection officials.

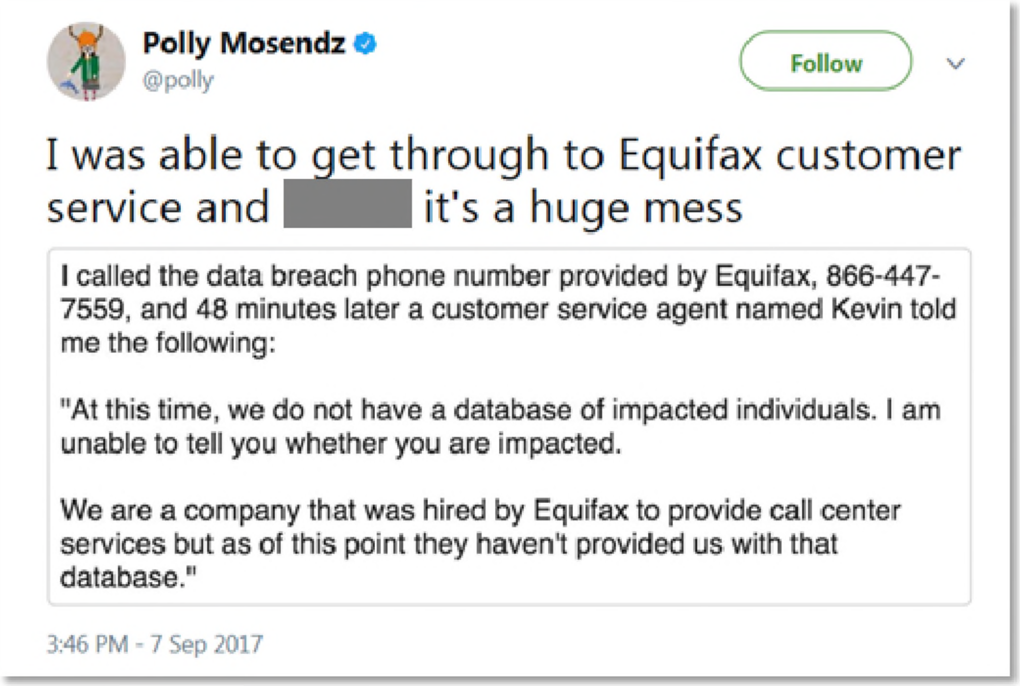
44. Aside from potentially luring victims into jeopardizing their right to sue, the Equifax website did not provide victims useful information on which they could act to protect their identities. Some victims who checked the website and

were told they had not been affected were given the opposite answer when they checked later on a phone using the same information.

45. For example, entering two made-up identities—last names "Smith" and "Doe," both with the last six Social Security number digits "123456"—yielded the same response:


Thank You
Based on the information provided, we believe that your personal information may have been impacted by this incident.
Click the button below to continue your enrollment in TrustedID Premier.
Enroll
For more information visit the FAQ page.

46. Those victims who called the hotline set up to aid Equifax victims fared little better. They were greeted by unprepared customer service agents without any helpful information. This complaint provides one example:


Polly Mosendz
@polly
Follow

I was able to get through to Equifax customer service and [redacted] it's a huge mess

I called the data breach phone number provided by Equifax, 866-447-7559, and 48 minutes later a customer service agent named Kevin told me the following:

"At this time, we do not have a database of impacted individuals. I am unable to tell you whether you are impacted.

We are a company that was hired by Equifax to provide call center services but as of this point they haven't provided us with that database."

3:46 PM - 7 Sep 2017

47. Even now, weeks after the Data Breach, Equifax has not been able to provide Americans definitive answers about whether or not their most sensitive personal information has been exposed.

48. If a victim set up a credit freeze—one recommended, potentially expensive and time-consuming prophylactic—Equifax provided a 10-digit personal identification number ("PIN"). Such PINs are supposed to be difficult to guess, but the PINs Equifax is providing are based on the time and date the person set up a freeze; thus, undercutting one of the key tools victims can use to prevent identify theft.

49. In at least one instance, when a frustrated Equifax customer who had previously enrolled in Equifax's paid monitoring service sought help online, Equifax directed them to a fake "phishing" website, securityequifax2017:

Equifax Inc.
@Equifax
Follow
Replying to @eqloprtntyhtr
Hi! For more information about the product and enrollment, please visit: securityequifax2017.com. -Tim
3:11 PM - 19 Sep 2017
18 Retweets 54 Likes
43
18
54

50. The website to which Equifax directed the consumer was critical of Equifax for using a domain name that could be so easily impersonated by phishing sites, leaving "millions vulnerable to phishing attacks on copycat sites":

EQUIFAX
Return to equifax.com
To enroll in complimentary identity theft protection and credit file monitoring, click here.
Cybersecurity Incident & Important Consumer Information Which is Totally Fake, Why Did Equifax Use A Domain That's So Easily Impersonated By Phishing Sites?
Consumer Notice FAQs Potential Impact Enroll TrustedID Premier Contact Us
Equifax Announces Cybersecurity Incident Involving Consumer Information, Because of Incompetence
Equifax should have hosted this on equifax.com with a reputable [EV] SSL Certificate.
Instead they chose an easily impersonated domain and used a jelly-bean SSL cert that any script kiddie can impersonate in 20min.
Their response to this incident leaves millions vulnerable to phishing attacks on copycat sites.
This is why you don't put your security incident website on a domain that looks like a scam (with an Amazon SSL cert), no-one can tell the difference between the real thing an a phishing site. Try the form by clicking "Potential Impact"
Rick Smith, Chairman and CEO of Equifax, on Cybersecuri...

C. Equifax's Failures Have Harmed and Will Continue to Harm Breach Victims

51. While Equifax's response to the Data Breach has been almost comically inept, the harm for victims is terribly serious. As a result of the Data Breach, criminals now have access to the essential building blocks to steal the identities of 143 million Americans, roughly 44 percent of the population.

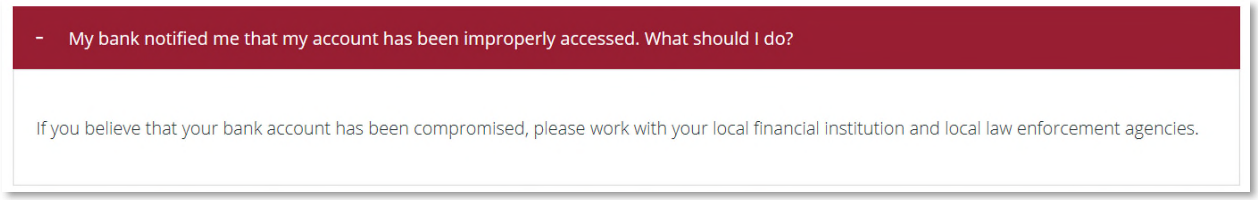
52. The Equifax Data Breach has greatly increased the victims' risk of identity theft relative to the time before the Data Breach. Unlike the credit and debit card numbers stolen in some of the other recent high-profile data breaches,

much of the information furnished here cannot simply be changed, and will continue to be valuable to identity thieves for many years.

53. As the Government Accountability Office reported in 2012, individuals who experience a data breach involving their Social Security number and dates of birth experience a much higher likelihood of being a victim of an identity crime. Social Security numbers, dates of birth, and names "are among the three personal identifiers most often sought by identity thieves," according to the GAO.

54. The Equifax Data Breach released all those personal identifiers, putting victims at increased risk of credit/debit card fraud, financial identity theft, tax fraud/identity theft, account takeovers, social identity fraud, and other harms.

55. Equifax's website for providing information to Data Breach victims acknowledges that they may already have experienced identity theft, including an answer for people who have been notified by their bank that their account "has been improperly accessed":


- My bank notified me that my account has been improperly accessed. What should I do?
If you believe that your bank account has been compromised, please work with your local financial institution and local law enforcement agencies.

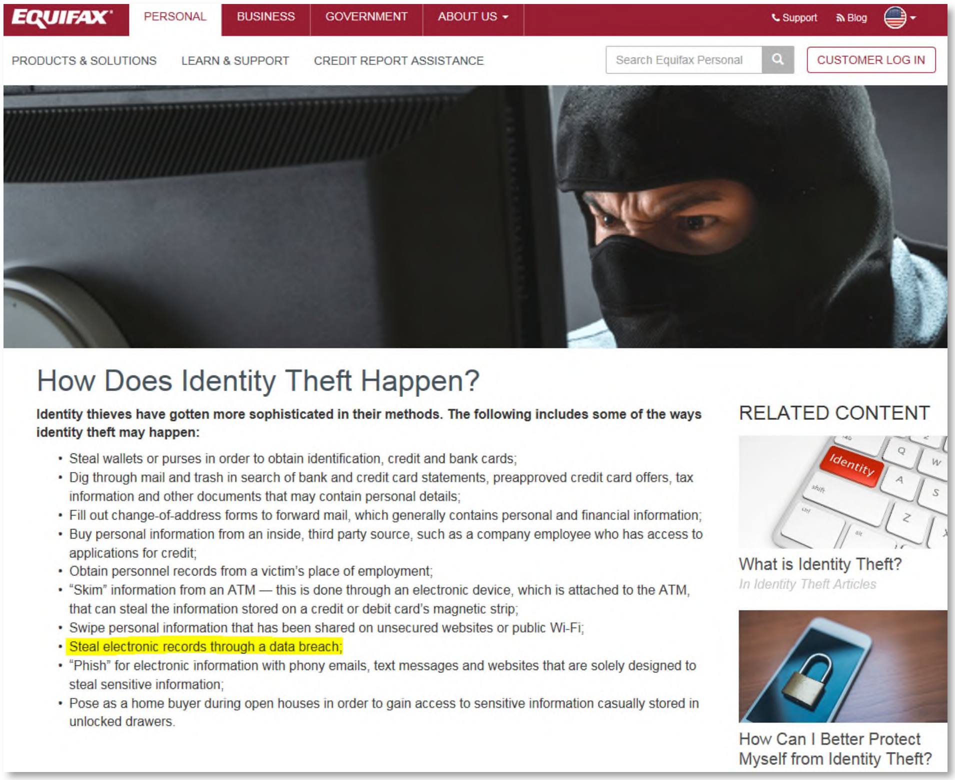
56. The same website recommends that victims "remain vigilant for incidents of fraud and identity theft[.]"

57. Equifax was aware of the increased risk of identity theft that data breaches cause, and the impacts of that identity theft. In fact, it appears that the hackers stole the credit card information, Social Security numbers, and addresses of over 200,000 individuals who had signed up for credit monitoring services through Equifax.

58. Equifax has published a pamphlet called "A Lasting Impact: The Emotional Toll of Identity Theft" discussing the "real" impacts that identity theft victims face, which advises that to avoid identify theft people should keep their Social Security numbers, drivers licenses, and addresses private.

59. Elsewhere, Equifax explained that to protect themselves from identify theft, people should "[k]eep your personal information secure online" and "[s]ecure your Social Security Number."

60. One way identify theft could happen, Equifax warned, was the theft "of electronic records through a data breach":


EQUIFAX
PERSONAL
BUSINESS
GOVERNMENT
ABOUT US
Support
Blog
PRODUCTS & SOLUTIONS
LEARN & SUPPORT
CREDIT REPORT ASSISTANCE
Search Equifax Personal
CUSTOMER LOG IN
How Does Identity Theft Happen?
Identity thieves have gotten more sophisticated in their methods. The following includes some of the ways identity theft may happen:
• Steal wallets or purses in order to obtain identification, credit and bank cards;
• Dig through mail and trash in search of bank and credit card statements, preapproved credit card offers, tax information and other documents that may contain personal details;
• Fill out change-of-address forms to forward mail, which generally contains personal and financial information;
• Buy personal information from an inside, third party source, such as a company employee who has access to applications for credit;
• Obtain personnel records from a victim's place of employment;
• "Skim" information from an ATM — this is done through an electronic device, which is attached to the ATM, that can steal the information stored on a credit or debit card's magnetic strip;
• Swipe personal information that has been shared on unsecured websites or public Wi-Fi;
• Steal electronic records through a data breach;
• "Phish" for electronic information with phony emails, text messages and websites that are solely designed to steal sensitive information;
• Pose as a home buyer during open houses in order to gain access to sensitive information casually stored in unlocked drawers.
RELATED CONTENT
Identity
What is Identity Theft?
In Identity Theft Articles
How Can I Better Protect Myself from Identity Theft?

61. Equifax has also acknowledged the increased risk that victims face by offering victims a one-year trial period of its proprietary credit monitoring service, TrustedID. But victims' increased risk of identity theft will last far beyond that one-year period. Identity thieves commonly wait years to commit fraud using breached data.

62. While victims are left vulnerable to identify theft, three top Equifax executives may have cashed out on the Data Breach, reportedly selling millions of dollars of stock after the company became aware of the breach but before the public found out.

V. CLASS ACTION ALLEGATIONS

A. Class Definition(s)

1. National Class

63. Pursuant to Fed. R. Civ. P. 23(a), (b)(2), (b)(3) and (c)(4), Plaintiffs seek relief on behalf of themselves and as representatives of a proposed nationwide class ("Nationwide Class"), defined as follows:

> All natural persons in the United States whose personally identifying information ("PII") was compromised as a result of the Data Breach.

2. Statewide Classes

64. Pursuant to Fed. R. Civ. P. 23, Plaintiffs assert claims under the laws of individual states, and on behalf of separate statewide subclasses, for each of the following states:

a. California

b. Virginia

c. New Jersey

d. Washington

e. District of Columbia

f. Pennsylvania

g. Delaware

h. Florida

i. South Carolina

j. Georgia

k. Louisiana

l. Missouri

m. Alabama

Each proposed statewide class ("Statewide Class") is defined as follows:

> All natural persons who are citizens of [STATE] whose PII was compromised as a result of the Data Breach.

65. Except where otherwise noted, "Class" or "Class members" shall refer to members of the Nationwide Class and each of the Statewide Classes.

66. Excluded from the Class are Defendant and any of its affiliates, parents or subsidiaries; all employees of Defendant; as well as the Court and its personnel presiding over this action.

67. Numerosity. The proposed Class is sufficiently numerous, as 143 million Data Breach victims had their PII compromised, and they are dispersed throughout the United States, making joinder of all members impracticable. Class members can be readily identified and ascertained through the records maintained by Equifax.

68. Commonality. Common questions of fact and law exist for each cause of action and predominate over questions affecting only individual class members, including:

a. Whether Equifax had a legal duty to use reasonable security measures to protect Class members' PII;

b. Whether Equifax timely, accurately, and adequately informed Class members that their PII had been compromised;

c. Whether Equifax breached its legal duty by failing to protect Class members' PII;

d. Whether Equifax acted reasonably in securing Class members' PII;

e. Whether Class members are entitled to actual damages and/or statutory damages; and

f. Whether Class members are entitled to injunctive relief.

69. **Typicality.** Plaintiffs' claims are typical of the claims of members of the proposed Class because, among other things, Plaintiffs and Class members sustained similar injuries as a result of Equifax's uniform wrongful conduct and their legal claims all arise from the same conduct by Equifax.

70. **Adequacy.** Plaintiffs will fairly and adequately protect the interests of the proposed Class. Plaintiffs' interests do not conflict with other Class members' interests and they have retained counsel experienced in complex class action and data privacy litigation to prosecute this case on behalf of the Class.

71. **Rule 23(b)(3).** In addition to satisfying the prerequisites of Rule 23(a), Plaintiffs satisfy the requirements for maintaining a class action under Rule 23(b)(3). Common questions of law and fact predominate over any questions affecting only individual Class members and a class action is superior to individual litigation. The amount of damages available to individual plaintiffs is insufficient to make litigation addressing Equifax's conduct economically feasible in the absence of the class action procedure. Individualized litigation also presents a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system presented by the legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

72. **Rule 23(b)(2).** Plaintiffs also satisfy the requirements for maintaining a class action under Rule 23(b)(2). Equifax has acted or refused to act on grounds that apply generally to the proposed Class, making final declaratory or injunctive relief appropriate with respect to the proposed Class as a whole.

73. **Rule 23(c)(4).** This action also satisfies the requirements for maintaining a class action under Rule 23(c)(4). The claims of Class members are

composed of particular issues that are common to all Class members and capable of class wide resolution that will significantly advance the litigation.

VI. CLAIMS FOR RELIEF

Claims Asserted on Behalf of the Nationwide Class:

COUNT I — Willful Violation of The Fair Credit Reporting Act, 15 U.S.C. §§ 1681 et seq.

1. Overview

74. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

75. Plaintiffs and the Class bring this claim to recover damages suffered as a result of Equifax's below-described willful violations of the Fair Credit Reporting Act (herein, "FCRA" or "the Act"), 15 U.S.C. §§ 1681 et seq.

76. As individuals, Plaintiffs and Nationwide Class members are consumers entitled to the protections of FCRA. 15 U.S.C. § 1681a(c).

77. Congress, in enacting FCRA, found that "[c]onsumer reporting agencies," like Equifax, "have assumed a vital role in assembling and evaluating consumer credit and other information on consumers" and, as a result, "[t]here is a need to insure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy." 15 U.S.C. § 1681(a)(3)-(4) (emphasis added).

78. Under FCRA, a "consumer reporting agency" is defined as "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties . . . ." 15 U.S.C. § 1681a(f).

79. Equifax is a consumer reporting agency under FCRA because it, for monetary fees, regularly engages in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties.

80. Congress further noted that one purpose of the Act is to "require that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information." *See* 15 U.S.C. § 1681(b) (emphasis added).

81. As detailed below, Equifax failed to fulfill its statutory obligations under the Act by, at a minimum: (a) failing to adopt reasonable procedures to protect the confidentiality, privacy, and proper utilization of Plaintiffs' and the Nationwide Class members' personal consumer, credit, and other personally-

identifying information including names, social security numbers, credit card numbers, account numbers, credit histories and other credit data; (b) furnishing and/or disclosing that information to improper third parties; (c) failing to take swift action upon learning of unauthorized access to Plaintiffs' and the Nationwide Class members' personal information and its unauthorized dissemination to third parties; and (d) disclosing, exposing, and/or making known to unauthorized third parties, the medical information of Plaintiffs and Nationwide Class members.

2. Violations of 15 U.S.C. § 1681e(a) – Willful Failure to Maintain Reasonable Security Measures

82. 15 U.S.C. § 1681e(a) requires that "consumer reporting agenc[ies]," such as Equifax, "shall maintain reasonable procedures designed to avoid violations of section 1681c of this title and to limit the furnishing of consumer reports to the purposes listed under [15 U.S.C. § 1681b]." 15 U.S.C. § 1681e(a).

83. These procedures, the Act goes on to explain: "shall require that prospective users of the information identify themselves, certify the purposes for which the information is sought, and certify that the information will be used for no other purpose." *Id*.

84. Moreover, the Act directs that "[n]o consumer reporting agency may furnish a consumer report to any person if it has reasonable grounds for believing

that the consumer report will not be used for a [permissible] purposed listed in section 1681b of this title." *Id.*

85. The Federal Trade Commission has explained that 15 U.S.C.§ 1681e(a) requires consumer reporting agencies to "have reasonable and effective procedures to limit unauthorized access to its databases. Such procedures may include a system of monitoring access to its database of consumer reports, including a system to monitor anomalies and other suspicious activity to guard against unauthorized access . . . . Procedures also may include . . . installation and use of appropriate computer hardware and software. . . ." Fed. Trade Comm'n, 40 Years of Experience with the Fair Credit Reporting Act at 66 (July 2011).

86. And, the Federal Trade Commission ("FTC") has pursued enforcement actions against consumer reporting agencies under the FCRA for failing "take adequate measures to fulfill their obligations to protect information contained in consumer reports, as required by the" FCRA, in connection with data breaches.

87. Equifax violated Section 1681e(a) by failing to implement and maintain reasonable, industry-standard security measures to ensure that Plaintiffs' and the Nationwide Class members' consumer credit information was not accessed for an impermissible purpose.

88. Equifax further violated Section 1681e(a) by failing to require prospective users of information to identify themselves as well as their purpose before permitting them access to Plaintiffs' and the Nationwide Class members' consumer credit information.

89. Equifax's failure to adopt and maintain such protective procedures directly and proximately resulted in the theft of and improper access to Plaintiffs' and the Nationwide Class members' consumer and credit information as well as its wrongful dissemination to unauthorized third parties in the public domain.

3. Violations of 15 U.S.C. § 1681b(a) – Furnishing Consumer Data Without a Permissible Purpose

90. 15 U.S.C. § 1681b provides that a "consumer reporting agency," like Equifax, "may furnish a consumer report under the following circumstances and no other:" (1) in response to a court order; (2) in response to a consumer request; (3) to a person which it has reason to believe will use the information for a credit, employment, insurance, licensing, or other legitimate business purpose; and (4) in response to a request by a government agency. *Id*.

91. FCRA defines a "consumer report" as: "[A]ny written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to

be used or collected in whole or in part for the purpose of establishing the consumer's eligibility for credit or insurance to be used primarily for personal, family, or household purposes; employment purposes, or any other purpose authorized under [15 U.S.C. §] 1681(b)." 15 U.S.C. § 1681a(d)(1).

92. Plaintiffs' and the Nationwide Class members' personally-identifying and other consumer information including their names, social security numbers, credit card numbers, account numbers, credit history, and other credit data constitute a "consumer report" within the meaning of 15 U.S.C. § 1681a(d)(1) because that information bears on their credit-worthiness, personal characteristics, and character and was collected by Equifax for the purpose of establishing their eligibility for credit.

93. Equifax violated § 1681b by furnishing and/or providing a written, oral, or other communications and/or documents and files which contained Plaintiffs' and the Nationwide Class members' personally-identifying and other consumer information to unauthorized third parties, who Equifax had no reason to believe would use the information for a permissible purpose.

4. Violations of 15 U.S.C. § 1681b(g) – Willful Disclosure of Confidential Medical Data

94. In addition to ensuring the protection of personal consumer credit data, FCRA lays out special requirements for consumer reporting agencies with

respect to confidential medical information, and restricting its dissemination or disclosure. *See, e.g.*, 15 U.S.C. §§ 1681a(d)(3); 1681b(g); 1681 c(a)(6).

95. Upon information and belief Equifax maintains “medical information” as a component of its effort to assess the credit-worthiness of consumers. Indeed, according to a review published by the Federal Reserve, nearly half of debt collection tradelines on credit reports are for medical debts. *See* Robert Avery, Paul Calem, Glenn Canner, & Raphael Bostic, An Overview of Consumer Data and Credit Reporting, Fed. Reserve Bulletin (RB), p. 69 (Feb. 2003).

96. Equifax violated § 1681b by disclosing, exposing, and/or making known to unauthorized third parties, the medical information of Plaintiffs and the Nationwide Class members, as detailed herein, and they were harmed as a result.

5. Violations of 15 U.S.C. § 1681c-1 – Willful Failure to Respond to Suspected Identify Theft

97. 15 U.S.C. § 1681c-1 imposes obligations on consumer reporting agencies like Equifax upon suspicion of fraud or identity theft.

98. Specifically, § 1681c-1 provides that “[u]pon the direct request of a consumer, or an individual acting on behalf of . . . of a consumer, who asserts in good faith a suspicion that the consumer has been or is about to become a victim of fraud or related crime, including identity theft, a consumer reporting agency shall . . . include a fraud alert in the file of that consumer . . . for a period of not less than

90 days . . . and refer the information regarding the fraud alert . . . to each of the other consumer reporting agencies," and provide certain disclosures to consumers as noted in §1681c-1(a)(2). *See* 15 U.S.C. § 1681c-1(a)(2).

99. On information and belief, Equifax was given notice of that fact that millions of consumers were at risk of becoming the victim of fraud and identity theft due to the unprecedented Data Breach described above, more than one month before it was made known to the public.

100. Nevertheless, and in violation of its obligations under 15 U.S.C. § 1681c-1, Equifax did not make timely disclosures to affected consumers, did not include fraud alerts to prevent identity theft following the Data Breach, and did not make timely notifications to other consumer reporting agencies; as a result, in addition to the harm described herein, Plaintiffs and the Nationwide Class were put at additional risk of fraud and identity theft, and were forced to incur additional costs to prevent the theft themselves.

6. Plaintiffs and the Nationwide Class Suffered Damages as a Proximate Result of Equifax's Willful Violations of FCRA and are Entitled to Relief

101. Equifax willfully violated the above-described provision of FCRA. The willful nature of Equifax's violations is supported by Equifax's other data breaches in the past. Further, Equifax touts itself as an industry leader in breach

prevention; thus, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, and willingly failed to take them.

102. Equifax also acted willfully because it knew or should have known about its legal obligations regarding data security and data breaches under the FCRA. These obligations are well established in the plain language of the FCRA and in the promulgations of the Federal Trade Commission. *See, e.g.*, 55 Fed. Reg. 18804 (May 4, 1990), 1990 Commentary On The Fair Credit Reporting Act. 16 C.F.R. Part 600, Appendix To Part 600, Sec. 607 2E. Equifax obtained or had available these and other substantial written materials that apprised it of its duties under the FCRA. Any reasonable consumer reporting agency knows or should know about these requirements. Despite knowing of these legal obligations, Equifax acted consciously in breaching known duties regarding data security and data breaches and depriving Plaintiffs and other members of the classes of their rights under the FCRA.

103. Equifax's willful and/or reckless conduct provided a means for unauthorized intruders to obtain and misuse Plaintiffs' and Nationwide Class members' personal information for no permissible purposes under the FCRA.

104. As a direct and proximate result of Equifax's willful violations of FCRA, and the resulting Data Breach described above, the personally-identifying and consumer credit information of Plaintiffs and the Nationwide Class members was stolen and made accessible to unauthorized third parties in the public domain.

105. As a direct and proximate result of Equifax's willful violations of FCRA, and the resulting Data Breach described above, Plaintiffs and Nationwide Class members were and continue to be damaged in the form of, without limitation, an increased cost of credit associated with misuse of their credit data, expenses for credit monitoring and identity theft insurance, other out-of-pocket expenses, anxiety, emotional distress, loss of privacy and other economic and non-economic harm.

106. As a result of Equifax's willful failure to "to comply with any requirement imposed under" the Act, it is liable to Plaintiffs and the Nationwide Class members for actual and statutory damages, together with their fees and costs. *See* 15 U.S.C. § 1681n (discussing willful noncompliance).

107. Plaintiffs and the Nationwide Class members, therefore, are entitled to compensation for their actual damages including, inter alia, (i) an increased cost of credit associated with misuse of their credit data; (ii) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and identity fraud pressed

upon them by the Data Breach described above; (iii) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (iv) deprivation of the value of their personally-identifying information, personal health information, and credit data for which there is a well-established national and international market; (v) anxiety and emotional distress; together with (vi) statutory damages of not less than $100, and not more than $1000, each; and (vii) attorneys' fees, litigation expenses and costs, pursuant to 15 U.S.C. § 1681n(a).

COUNT II —
NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT

108. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

109. Plaintiffs and the Nationwide Class bring this claim to recover damages suffered as a result of Equifax's below-described negligent violations of the Fair Credit Reporting Act (herein, "FCRA" or "the Act"), 15 U.S.C. §§ 1681 et seq.

110. As detailed above, as individuals, Plaintiffs and Nationwide Class members are consumers entitled to the protections of FCRA, 15 U.S.C. § 1681a(c), and 15 U.S.C. § 1681a(f).

111. Equifax is a consumer reporting agency under FCRA because it, for monetary fees, regularly engages in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties. 15 U.S.C. § 1681 a(f).

112. As detailed above, Equifax failed to fulfill its statutory obligations under the Act by, at a minimum: (a) failing to adopt reasonable procedures to protect the confidentiality, privacy, and proper utilization of Plaintiffs and the Nationwide Class members' personal consumer, credit, and other personally-identifying information including their names, social security numbers, credit card numbers, account numbers, credit histories and other credit data; (b) furnishing and/or disclosing that information to improper third parties; (c) failing to take swift action upon learning of unauthorized access to Plaintiffs and the Nationwide Class members' personal information and its unauthorized dissemination to third parties; and (d) disclosing, exposing, and/or making known to unauthorized third parties, the medical information of Plaintiffs and Nationwide Class members.

113. Specifically, Equifax violated FCRA by willfully and/or negligently (1) failing to adopt and maintain reasonable procedures to protect the confidentiality of consumer information in violation of 15 U.S.C. § 1681e; (2) furnishing and/or disclosing consumer information to unauthorized third parties

without a permissible purpose in violation of 15 U.S.C. § 1681b; (3) disclosing confidential medical information in violation of 15 U.S.C. §§ 1681b(g)(4), and 1681b(g)(3)(A); and (4) failing to respond to identity theft or the suspicion of identity theft in violation of 15 U.S.C. § 1681c-1.

114. 15 U.S.C. § 1681b provides that a "consumer reporting agency," like Equifax, "may furnish a consumer report under the following circumstances and no other:" (1) in response to a court order; (2) in response to a consumer request; (3) to a person which it has reason to believe will use the information for a credit, employment, insurance, licensing, or other legitimate business purpose; and (4) in response to a request by a government agency. *Id*.

115. FCRA defines a "consumer report" as: "[A]ny written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of establishing the consumer's eligibility for credit or insurance to be used primarily for personal, family, or household purposes; employment purposes, or any other purpose authorized under [15 U.S.C. §] 1681(b)." 15 U.S.C. § 1681a(d)(1).

116. Plaintiffs and the Nationwide Class members' personally-identifying and other consumer information including their names, social security numbers, credit card numbers, account numbers, credit history, and other credit data constitute a "consumer report" within the meaning of 15 U.S.C. § 1681a(d)(1) because that information bears on their credit-worthiness, personal characteristics, and character and was collected by Equifax for the purpose of establishing their eligibility for credit.

117. Equifax violated § 1681b by furnishing and/or providing a written, oral, or other communications and/or documents and files which contained Plaintiffs and the Nationwide Class members' personally-identifying and other consumer information to unauthorized third parties, who Equifax had no reason to believe would use the information for a permissible purpose.

118. Equifax negligently violated the above-described provision of FCRA. Equifax's negligent failure to maintain reasonable procedures is supported by Equifax's other data breaches in the past. Further, as an enterprise claiming to be an industry leader in data breach prevention, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, yet failed to take them.

119. Equifax's negligent conduct provided a means for unauthorized intruders to obtain and misuse Plaintiffs' and Nationwide Class members' personal information for no permissible purposes under FCRA.

120. As a direct and proximate result of Equifax's negligent violations of FCRA, and the resulting Data Breach described above, the personally-identifying and consumer credit information of Plaintiffs and the Nationwide Class members was stolen and made accessible to unauthorized third parties in the public domain.

121. As a direct and proximate result of Equifax's negligent violations of FCRA, and the resulting Data Breach described above, Plaintiffs and Nationwide Class members were and continue to be damaged in the form of, without limitation, an increased cost of credit associated with misuse of their credit data, expenses for credit monitoring and identity theft insurance, other out-of-pocket expenses, anxiety, emotional distress, loss of privacy and other economic and non-economic harm.

122. Plaintiffs and Nationwide Class members, therefore, are entitled to compensation for their actual damages including, inter alia, (i) an increased cost of credit associated with misuse of their credit data; (ii) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and identity fraud pressed upon them by the Data Breach described above; (iii) the value of their time spent

mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (iv) deprivation of the value of their personally-identifying information, personal health information, and credit data for which there is a well-established national and international market; (v) anxiety and emotional distress; together with (vi) attorneys' fees, litigation expenses and costs, pursuant to 15 U.S.C. § 1681o(a).

COUNT III — NEGLIGENCE

123. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

124. Equifax owed a duty to Plaintiffs and the Nationwide Class members to exercise reasonable care in safeguarding and protecting their highly sensitive and personal information. This duty included, among other things, designing, maintaining, monitoring, testing Equifax's security systems, protocols, and practices, as well as taking other reasonable security measures to protect and adequately secure the PII of Plaintiffs and Nationwide Class members from unauthorized access.

125. Equifax owed a duty to Class members to implement administrative, physical and technical safeguards, such as intrusion detection processes that detect

data breaches in a timely manner, to protect and secure Plaintiffs' and Nationwide Class members' PII.

126. Equifax owed a duty of care to Plaintiffs and Nationwide Class members because they were foreseeable and probable victims of any inadequate security practices. It was foreseeable that if Equifax did not take reasonable security measures, the PII of Plaintiffs and members of the Nationwide Class would be stolen. Major corporations, and particularly credit rating agencies, like Equifax face a higher threat of security breaches than smaller companies due in part to the large amounts of data they possess. Equifax knew or should have known its security systems were inadequate, particularly in light of the prior data breaches that Equifax had experienced, and yet Equifax failed to take reasonable precautions to safeguard the PII of Plaintiffs and members of the Nationwide Class.

127. Equifax owed a duty to disclose the material fact that its data security practices were inadequate to safeguard Nationwide Class members' PII.

128. Equifax had a duty to timely and accurately notify Plaintiffs and Nationwide Class members if their PII was compromised so that Plaintiffs and Nationwide Class members could act to mitigate the harm caused by the loss of opportunity to control how their PII was used.

129. Equifax breached its duties by, among other things: (a) failing to implement and maintain adequate data security practices to safeguard Nationwide Class members' PII; (b) failing to detect the Data Breach in a timely manner; (c) failing to disclose that Defendant's data security practices were inadequate to safeguard Nationwide Class members' PII; and (d) failing to provided adequate and timely notice of the breach.

130. But for Equifax's breach of its duties, Nationwide Class members' PII would not have been accessed by unauthorized individuals.

131. Plaintiffs and Nationwide Class members were foreseeable victims of Equifax's inadequate data security practices. Equifax knew or should have known that a breach of its data security systems would cause damages to Nationwide Class members.

132. Equifax's negligent conduct provided a means for unauthorized intruders to obtain Plaintiffs' and the Nationwide Class members' PII and consumer reports for no permissible purposes under FCRA.

133. As a result of Equifax's willful failure to prevent the Data Breach, Plaintiffs and Nationwide Class members suffered injury, which includes but is not limited to: (1) exposure to a heightened, imminent risk of fraud, identity theft, and financial harm; (2) the loss of the opportunity to control how their PII is used; (3)

the diminution in the value and/or use of their PII; (4) the compromise, publication, and/or theft of their PII; (5) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of financial accounts; (6) lost opportunity costs associated with the effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft, as well as the time and effort Plaintiffs and Nationwide Class members have expended to monitor their financial accounts and credit histories to guard against identity theft; (7) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased costs to use credit, credit scores, credit reports and assets; (8) unauthorized use of compromised PII to open new financial accounts; (9) tax fraud and/or other unauthorized charges to financial accounts and associated lack of access to funds while proper information is confirmed and corrected; (10) the continued risk to their PII, which remain in Equifax's possession and are subject to further breaches so long as Equifax fails to undertake appropriate and adequate measures to protect the PII in its possession; and (10) future costs in terms of time, effort and money that will be expended, to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives.

134. The damages to Plaintiffs and Nationwide Class members were a proximate, reasonably foreseeable result of Equifax's breaches of its duties.

135. Plaintiffs and the Nationwide Class are also entitled to damages and reasonable attorneys' fees and costs. Plaintiffs also seek reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23 and California Code of Civil Procedure § 1021.5.

COUNT IV —
NEGLIGENCE PER SE

136. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

137. Under FCRA, 15 U.S.C. § 1681e, Equifax is required to "maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section 1681b of this title." 15 U.S.C. § 1681e(a).

138. Under FCRA, 15 U.S.C. § 168b, a "consumer reporting agency," like Equifax, "may furnish a consumer report under the following circumstances and no other:" (1) in response to a court order; (2) in response to a consumer request; (3) to a person which it has reason to believe will use the information for a credit,

employment, insurance, licensing, or other legitimate business purpose; and (4) in response to a request by a government agency. *Id*.

139. Defendant failed to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of FCRA.

140. Under 15 U.S.C. § 1681c-1, FCRA imposes obligations on consumer reporting agencies like Equifax to make timely disclosures to consumers upon suspicion of fraud or identity theft.

141. Specifically, § 1681c-1 provides that "[u]pon the direct request of a consumer, or an individual acting on behalf of . . . of a consumer, who asserts in good faith a suspicion that the consumer has been or is about to become a victim of fraud or related crime, including identity theft, a consumer reporting agency shall . . . include a fraud alert in the file of that consumer . . . for a period of not less than 90 days . . . and refer the information regarding the fraud alert . . . to each of the other consumer reporting agencies," and provide certain disclosures to consumers as noted in § 1681c-1(a)(2). *See* 15 U.S.C. § 1681c-1(a)(2).

142. On information and belief, Equifax was given notice of the fact that millions of consumers were at risk of becoming the victim of fraud and identity

theft due to the unprecedented Data Breach described above, months before it was made known to the public.

143. Nevertheless, and in violation of its obligations under 15 U.S.C. § 1681c-1, Equifax did not make timely disclosures to affected consumers, did not include fraud alerts to prevent identity theft following the Data Breach, and did not make timely notifications to other consumer reporting agencies; as a result, in addition to the harm described herein, Plaintiffs and the Nationwide Class were put at additional risk of fraud and identity theft, and were forced to incur additional costs to prevent the theft themselves.

144. Under 15 U.S.C. §§ 1681a(d)(3); 1681b(g); 1681 c(a)(6), FCRA imposes requirements for consumer reporting agencies with respect to confidential medical information, and restricting its dissemination or disclosure. In violation of these obligations, Equifax disclosed, exposed, and/or made known to unauthorized third parties, the medical information of Plaintiffs and the Nationwide Class members.

145. Plaintiffs and the Nationwide Class members are within the class of persons that FCRA was intended to protect.

146. Plaintiffs and Nationwide Class members were foreseeable victims of Equifax's violation of FCRA. Equifax knew or should have known that a breach of its data security systems would cause injuries to Nationwide Class members.

147. Equifax likewise violated Section 5(a) of the FTC Act, which provides that 'unfair or deceptive acts or practices in or affecting commerce...are...declared unlawful." 15 U.S.C. § 45(a)(1).

148. By failing to use reasonable measures to protect consumers' PII and by not complying with applicable industry standards as discussed above, Equifax violated Section 5 of the FTC Act. Equifax's conduct was particularly unreasonable given the sensitive nature and vast amount of PII it had collected, obtained and stored, and the foreseeable consequences that a data breach of this information would substantially harm Plaintiffs and the Nationwide Class.

149. Equifax was required under the Gramm-Leach-Bliley Act ("GLBA") to satisfy certain standards relating to administrative, technical, and physical safeguards:

(1) to insure the security and confidentiality of customer records and information;

(2) to protect against any anticipated threats or hazards to the security or integrity of such records; and

(3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

150. In order to satisfy its obligations under the GLBA, Equifax was also required to "develop, implement, and maintain a comprehensive information security program that is [1] written in one or more readily accessible parts and [2] contains administrative, technical, and physical safeguards that are appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue." *See* 16 C.F.R. § 314.4

151. In addition, under the Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 225, App. F., Equifax had an affirmative duty to "develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems." *See id*.

152. Further, when Equifax became aware of "unauthorized access to sensitive customer information," it should have "conduct[ed] a reasonable investigation to promptly determine the likelihood that the information has been or will be misused" and "notif[ied] the affected customer[s] as soon as possible." *See id*.

153. Equifax violated the GLBA by failing to "develop, implement, and maintain a comprehensive information security program" with "administrative, technical, and physical safeguards" that were "appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue." This includes, but is not limited to, Equifax's failure to implement and maintain adequate data security practices to safeguard Nationwide Class members' PII; (b) failing to detect the Data Breach in a timely manner; and (c) failing to disclose that Defendant's data security practices were inadequate to safeguard Nationwide Class members' PII.

154. Equifax also violated the GLBA by failing to "develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems." This includes, but is not limited to, Equifax's failure to notify appropriate regulatory agencies, law enforcement, and the affected individuals themselves of the Data Breach in a timely and adequate manner.

155. Equifax also violated the GLBA by failing to notify affected consumers as soon as possible after it became aware of unauthorized access to sensitive customer information.

156. Plaintiffs and Nationwide Class members were foreseeable victims of Equifax's violation of the GLBA. Equifax knew or should have known that its failure to take reasonable measures to prevent a breach of its data security systems, and failure to timely and adequately notify the appropriate regulatory authorities, law enforcement, and Nationwide Class members themselves would cause damages to Nationwide Class members.

157. Defendant's failure to comply with the applicable laws and regulations, including FCRA, the FTC Act and the GLBA, constitutes negligence per se.

158. But for Equifax's violation of the applicable laws and regulations, Nationwide Class members' PII would not have been accessed by unauthorized individuals.

159. As a direct and proximate result of Equifax's negligence per se, Plaintiffs and the Nationwide Class members suffered, and continue to suffer, injuries, which include but are not limited to exposure to a heightened, imminent risk of fraud, identity theft, and financial harm. Plaintiffs and Nationwide Class members must more closely monitor their financial accounts and credit histories to guard against identity theft. Nationwide Class members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining

credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiffs and Nationwide Class members' PII has also diminished the value of their PII.

160. Therefore, Plaintiffs and Nationwide Class members are entitled to damages in an amount to be proven at trial.

COUNT V —
DECLARATORY JUDGMENT

161. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

162. As previously alleged, Plaintiffs and the Nationwide Class have stated claims against Equifax based on negligence and statutory violations.

163. Equifax has failed to live up to its obligations to provide reasonable security measures for the PII of Plaintiffs and the Nationwide Class.

164. Equifax still possesses PII pertaining to Plaintiffs and Nationwide Class members.

165. In addition, the Data Breach has rendered Equifax's system even more vulnerable to unauthorized access and requires that Equifax immediately take even more stringent measures to currently safeguard the PII of Plaintiffs and the Nationwide Class going forward.

166. Equifax has made no representation that it has remedied the vulnerabilities in its data security systems.

167. An actual controversy has arisen in the wake of the Data Breach regarding Equifax's current obligations to provide reasonable data security measures to protect the PII of Plaintiffs and the Nationwide Class. On information and belief, Equifax maintains that its security measures were, and remain, reasonably adequate. On information and belief, Equifax further denies that it previously had or now has any obligation to better safeguard the PII of Plaintiffs and the Nationwide Class.

168. Plaintiffs thus seek a declaration that to comply with its existing obligations, Equifax must implement specific additional, prudent industry security practices, as outlined below, to provide reasonable protection and security to the PII of Plaintiffs and the Nationwide Class.

169. Specifically, Plaintiffs and the class seek a declaration that (a) Equifax's existing security measures do not comply with its obligations, and (b) that to comply with its obligations, Equifax must implement and maintain reasonable security measures on behalf of Plaintiffs and the Nationwide Class, including, but not limited to: (1) engaging third party security auditors/penetration testers as well as internal security personnel to conduct testing consistent with

prudent industry practices, including simulated attacks, penetration tests, and audits on Equifax's systems on a periodic basis; (2) engaging third party security auditors and internal personnel to run automated security monitoring consistent with prudent industry practices; (3) auditing, testing, and training its security personnel regarding any new or modified procedures; (4) purging, deleting and destroying, in a secure manner, data not necessary for its business operations; (5) conducting regular database scanning and securing checks consistent with prudent industry practices; (6) periodically conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach consistent with prudent industry practices; (7) receiving periodic compliance audits by a third party regarding the security of the computer systems Equifax uses to store the personal information of Plaintiffs and the Nationwide Class members; (8) meaningfully educating Plaintiffs and the Nationwide Class members about the threats they face as a result of the loss of their PII to unauthorized third parties, as well as the steps they must take to protect themselves; and (9) providing ongoing identity theft protection, monitoring, and recovery services to Plaintiffs and Nationwide Class members.

7. Claims Asserted on Behalf of Statewide Classes

Claims Asserted on Behalf of the Georgia Statewide Class

COUNT VI —
Violation of the Georgia Uniform Deceptive Trade Practices Act, O.C.G.A. §§ 10-1-370 et seq.

170. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

171. Plaintiffs Hollie Moore and Jeffrey Warren Dixon bring this cause of action on behalf of the Georgia Statewide Class.

172. Plaintiffs and Equifax are persons within the meaning of O.C.G.A. § 10-1-371.

173. The Georgia UDTPA prohibits any “deceptive trade practices,” which include misrepresenting the “standard, quality, or grade” of goods or services, and engaging “in any other conduct which similarly creates a likelihood of confusion or of misunderstanding.” Ga. Code. Ann. § 10-1-372(a).

174. Plaintiffs and Georgia Statewide Class members entrusted Equifax with their PII.

175. As alleged herein, Equifax engaged in unfair or deceptive acts or practices in the conduct of consumer transactions, including the following, in violation of the GUDPTA:

- Failure to maintain adequate information security systems and data security practices to safeguard PII belonging to Plaintiffs and Georgia Statewide Class members;
- Failure to disclose that its information security systems and data security practices were inadequate to safeguard PII from theft;
- Failure to timely and accurately disclose the Data Breach to Plaintiffs and Georgia Statewide Class members;
- Representing that Equifax's information security systems and practices have characteristics or benefits that they do not have;
- Causing likelihood of confusion or of misunderstanding as to security of Plaintiffs' and Georgia Statewide Class members' sensitive information;
- Engaging in other misleading conduct which created a likelihood of confusion or of misunderstanding.
- Continued acceptance of PII and storage of other personal information after Equifax knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach; and
- Continued acceptance of PII and storage of other personal information after Equifax knew or should have known of the Data Breach and before it allegedly remediated the Breach.

176. As alleged above, Equifax's failure to secure consumers' PII violates the FTCA and therefore violates the GUDTPA.

177. Defendant had an ongoing duty to Plaintiffs and the Georgia Statewide Class to refrain from misleading and deceptive practices in the course of its business under Georgia's Consumer Protection from Deceptive Acts and Practices Law. Specifically, Defendant owed Plaintiffs and Georgia Statewide

members a duty to safeguard Plaintiffs' and the Georgia Statewide Class members sensitive data, to implement state-of-the-art cyber security controls, and to disclose all the material facts concerning its information security systems and practices because Defendant possessed exclusive knowledge with regard to the security of its systems; yet, intentionally concealed this knowledge from Plaintiffs and the Georgia Statewide Class, and/or made misrepresentations that were rendered misleading because they were contradicted by withheld facts.

178. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard the PII of Plaintiffs and Georgia Statewide Class members, deter hackers, and that the risk of a data breach was highly likely. Furthermore, Defendant knew that, as consumers, Plaintiffs and Georgia Statewide Class members would rely upon its deceptive and misleading conduct and could not have discovered the breach on their own.

179. As a direct and proximate result of Equifax's violation of GFBPA, Plaintiffs and Georgia Statewide Class members suffered damages including, but not limited to: an increased cost of credit associated with misuse of their credit data, expenses for credit monitoring and identify theft insurance, other out-of-pocket expenses, anxiety, emotional distress, loss of privacy and other economic and non-economic harm.

180. In addition, Equifax violated the O.C.G.A. § 10-1-912(a) by failing to notify Plaintiffs and Georgia Statewide Class members of the Data Breach in "the most expedient time possible and without unreasonable delay." Furthermore, Equifax failed to provide Plaintiffs and Georgia Statewide Class members with even the required minimum information for determining the scope of the Data Breach.

181. Defendant's violations present a continuing risk to Plaintiffs and the Georgia Statewide Class, as well as to the general public. Defendant's unlawful acts and practices complained of herein affect the public interest.

182. Defendant's unlawful actions have caused and are continuing to cause injury and damages to Plaintiffs and Georgia Statewide Class members. Pursuant to the GUDTPA, Plaintiffs and Statewide Georgia Class members are entitled to injunctive relief, including, but not limited to enjoining Defendant's unlawful and deceptive acts as set forth above, and such other relief as the Court deems just and proper, including restitutionary disgorgement.

183. Pursuant to O.C.G.A. § 10-1-373, Plaintiffs and Statewide Georgia Class members seek reasonable attorneys' fees and expenses incurred in connection with this action.

COUNT VII —
Violation of the Georgia Security Breach Notification Act, O.C.G.A. §§ 10-1-912 et seq.

184. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

185. Plaintiffs Hollie Moore and Jeffrey Warren Dixon bring this cause of action on behalf of the Georgia Statewide Class.

186. Under Ga. Code Ann. § 10-1-912(a), "[a]ny information broker … that maintains computerized data that includes personal information of individuals shall give notice of any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The notice shall be made in the most expedient time possible and without unreasonable delay … ."

187. Under Ga. Code Ann. § 10-1-912(b), "[a]ny person or business that maintains computerized data on behalf of an information broker … that includes personal information of individuals that the person or business does not own shall notify the information broker … of any breach of the security of the system within 24 hours following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

188. Equifax is an information broker that owns or licenses computerized data that includes personal information, as defined by Ga. Code Ann. § 10-1-911.

189. In the alternative, the Equifax maintains computerized data on behalf of an information broker that includes personal information that Equifax does not own, as defined by Ga. Code Ann. § 10-1-911.

190. Plaintiff and the Georgia Statewide Class members' PII (including but not limited to names, addresses, and Social Security numbers) includes personal information covered under Ga. Code Ann. § 10-1-911(6).

191. Because Equifax was aware of a breach of its security system (that was reasonably likely to have caused unauthorized persons to acquire Plaintiff and Class member' Personal Information), Equifax had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Ga. Code Ann. § 10-1-912(a).

192. By failing to disclose the Data Breach in a timely and accurate manner, Equifax violated Ga. Code Ann. § 10-1-912(a).

193. As a direct and proximate result of Equifax's violations of Ga. Code Ann. § 10-1-912(a), Plaintiffs and Class members suffered the damages alleged herein.

194. Plaintiffs and the Georgia Statewide Class members seek relief under Ga. Code Ann. § 10-1-912 including, but not limited to, actual damages and injunctive relief.

Claims Asserted on Behalf of the California Statewide Class

COUNT VIII —
Violation of the California Customer Records Act
California Civil Code Section 1798.80 et seq.

195. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

196. Plaintiffs Steven B. Stein and John Corona bring this cause of action on behalf of the California Statewide Class.

197. The California Legislature enacted Civil Code section 1798.81.5 "to ensure that personal information about California residents is protected." The statute requires that any business that "owns, licenses, or maintains personal information about a California resident … implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

198. Equifax is a "business" as defined by Civil Code section 1798.80(a).

199. Each Plaintiff and member of the California Statewide Class is an "individual" as defined by Civil Code section 1798.80(d).

200. The information taken in the Data Breach was "personal information" as defined by Civil Code sections 1798.80(e) and 1798.81.5(d), which includes "information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information."

201. The breach of the personal information of over 140,000 consumers was a "breach of the security system" of Equifax as defined by Civil Code section 1798.82(g).

202. By failing to implement reasonable security measures appropriate to the highly sensitive and confidential nature of consumers' personal information, Equifax violated Civil Code section 1798.81.5.

203. In addition, by failing to immediately notify all affected consumers that their personal information had been acquired (or was reasonably believed to

have been acquired) by unauthorized persons in the Data Breach, Equifax violated Civil Code section 1798.82 of the same title. Equifax's failure to immediately notify consumers of the breach caused California Statewide Class members to suffer damages because they have lost the opportunity to immediately: (i) buy identity protection, monitoring, and recovery services; (ii) flag asset, credit, and tax accounts for fraud, including reporting the theft of their Social Security numbers to financial institutions, credit agencies, and the Internal Revenue Service; (iii) purchase or otherwise obtain credit reports; (iv) monitor credit, financial, utility, explanation of benefits, and other account statements on a monthly basis for unrecognized credit inquiries, Social Security numbers, home addresses, charges; (v) place and renew credit fraud alerts on a quarterly basis; (vi) routinely monitor public records, loan data, or criminal records; (vii) contest fraudulent charges and other forms of criminal, financial identity theft, and repair damage to credit and other financial accounts; and (viii) take other steps to protect themselves and recover from identity theft and fraud.

204. Because it violated Civil Code sections 1798.81.5 and 1798.82, Equifax "may be enjoined" under Civil Code section 1798.84(e).

205. Plaintiffs request that the Court enter an injunction requiring Equifax to implement and maintain reasonable security procedures to protect California

Statewide Class members' PII, including, but not limited to, ordering that Equifax: (1) engage third party security auditors/penetration testers as well as internal security personnel to conduct testing consistent with prudent industry practices, including simulated attacks, penetration tests, and audits on Equifax's systems on a periodic basis; (2) engage third party security auditors and internal personnel to run automated security monitoring consistent with prudent industry practices; (3) audit, test, and train its security personnel regarding any new or modified procedures; (4) purge, delete and destroy, in a secure manner, data not necessary for its business operations; (5) conduct regular database scanning and securing checks consistent with prudent industry practices; (6) periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach consistent with prudent industry practices; (7) receive periodic compliance audits by a third party regarding the security of the computer systems Equifax uses to store consumers' personal information; (8) meaningfully educate Plaintiffs and California Statewide Class members about the threats they face as a result of the loss of their PII to unauthorized third parties, as well as the steps they must take to protect themselves; and (9) provide ongoing identity theft protection, monitoring, and recovery services to Plaintiffs and California Statewide Class members.

206. Plaintiffs further request that the Court order Equifax to (1) identify and notify all members of the class who have not yet been informed of the Data Breach; and (2) notify affected consumers of any future data breaches by email within 24 hours of Equifax's discovery of a breach or possible breach and by mail within 72 hours.

207. As a result of Equifax's violations of Civil Code sections 1798.81.5 and 1798.82, Plaintiffs and members of the California Statewide Class have incurred and will incur damages, including but not necessarily limited to: (1) the loss of the opportunity to control how their PII is used; (2) the diminution in the value and/or use of their PII; (3) the compromise, publication, and/or theft of their PII; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft; (5) lost opportunity costs associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity data misuse; (6) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased costs to use credit, credit scores, credit reports and assets; (7) unauthorized use of compromised PII to open new financial accounts; (8) tax fraud and/or other unauthorized charges to

financial accounts and associated lack of access to funds while proper information is confirmed and corrected; (9) the continued risk to their PII, which remain in Equifax's possession and are subject to further breaches so long as Equifax fails to undertake appropriate and adequate measures to protect the PII in its possession; and (10) future costs in terms of time, effort and money that will be expended, to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of the California Statewide Class members.

208. Plaintiffs seek all remedies available under Civil Code section 1798.84, including actual and statutory damages, equitable relief, and reasonable attorneys' fees. Plaintiffs also seek reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23 and California Code of Civil Procedure § 1021.5.

COUNT IX —
Violation of California's Unfair Competition Law, California Business and Professions Code Section 17200 et seq.

209. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

210. Plaintiffs Stein and Corona bring this cause of action on behalf of the California Statewide Class.

211. California's Unfair Competition Law ("UCL"), California Business & Professions Code §§ 17200 et seq., provides for relief where a defendant's acts, omissions, and practices are shown to be unlawful, unfair, and fraudulent. Equifax's acts, omissions, and practices constitute unlawful and unfair business practices in violation of the UCL.

212. Equifax's acts, omissions, and practices constitute unlawful practices and in violation of the Customer Records Act, FCRA, the FTC Act, California Civil Code §§ 1572, 1573, 1709, 1711, 1798.82, 1798.84; California Business & Professions Code §§ 17200 et seq.; California Business & Professions Code §§ 17500 et seq., and California common law because Equifax failed to take adequate security measures in protecting the confidentiality of Plaintiffs' and the California Statewide Class members' PII, Equifax unreasonably delayed informing Plaintiff and the California Statewide Class about the Data Breach, and Equifax negligently released Plaintiffs' and California Statewide Class members' PII that was within its possession and control.

213. Equifax's acts, omissions, and conduct constitute unlawful practices because it failed to comport with a reasonable standard of care and public policy as reflected in statutes such as the Information Practices Act of 1977, the Customer Records Act, FCRA, and FTC Act which seek to protect individuals' data and

ensure that entities who solicit or are entrusted with personal or medical data utilize reasonable data security measures. Equifax engaged in conduct that undermines or violates the stated policies underlying the California Customer Records Act and other privacy statutes. For instance, in enacting the Customer Records Act, the California Legislature stated that "[i]dentity theft is costly to the marketplace and to consumers" and that "victims of identity theft must act quickly to minimize the damage; therefore, expeditious notification of possible misuse of a person's personal information is imperative." 2002 Cal. Legis. Serv. Ch. 1054 (A.B. 700) (WEST). Similarly, the Information Practices Act of 1977 was enacted to protect individuals' data and ensure that entities who solicit or are entrusted with personal data use reasonable security measures.

214. Equifax's acts, omissions, and conduct also constitute unfair business acts or practices because they offend public policy and constitute immoral, unethical, and unscrupulous activities that caused substantial injury, including to Plaintiffs and California Statewide Class members. The gravity of harm resulting from Equifax's conduct outweighs any potential benefits attributable to the conduct and there were reasonably available alternatives to further Equifax's legitimate business interests. Equifax's conduct undermines public policy reflected in statutes such as FCRA and the FTC Act.

215. Equifax's acts, omissions, and conduct further constitute unfair business acts or practices because Plaintiffs and California Statewide Class members have been substantially injured by the negligent release of their PII, which outweighs any countervailing benefits to Plaintiffs and California Statewide Class members.

216. Equifax engaged in fraudulent business acts or practices by representing to Plaintiffs and California Statewide Class members that it maintains adequate data security practices and procedures to safeguard PII from unauthorized disclosure, release, data breaches, and theft, and that it would comply with relevant federal and state laws pertaining to the privacy and security of PII. Had Plaintiff sand California Statewide Class members known about Equifax's substandard data security practices, they would have taken steps to protect themselves from harm that could result from Equifax's substandard data security practices.

217. Equifax engaged in fraudulent business acts or practices by omitting, suppressing, and concealing the material fact of the inadequacy of the data security protections for the PII of Plaintiffs and California Statewide Class members. Equifax failed to disclose to Plaintiffs and California Statewide Class members that Equifax's computer systems and data security practices and measures failed to meet legal and industry standards, were inadequate to safeguard their PII and that

the risk of data breach or theft was highly likely. Had Plaintiffs and California Statewide Class members known about Equifax's substandard data security practices, they would have taken steps to protect themselves from harm that could result from Equifax's substandard data security practices.

218. Equifax's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and California Statewide Class members. Equifax's failure to disclose such material information rendered its representations of its data security practices as likely to deceive a reasonable consumer. Equifax knew such facts would (a) be unknown to and not easily discoverable by Plaintiffs and members of the California Statewide Class; and (b) defeat Plaintiff's and the California Statewide Class members' ordinary, foreseeable and reasonable expectations concerning the security of Equifax's data systems.

219. An objective, reasonable person would have been deceived by Equifax's representations about the security and protection of data in its databases and networks.

220. As a direct and proximate result of Equifax's unlawful, unfair, and fraudulent business practices, Plaintiffs and members of the California Statewide Class have suffered injury in fact, and are therefore entitled to relief, including

restitution, declaratory relief, and a permanent injunction enjoining Equifax from its unlawful and unfair practices. Equifax's conduct caused and continues to cause substantial injury to Plaintiffs and California Statewide Class members. Equifax will continue to maintain Plaintiffs' and California Statewide Class members' PII for the indefinite future. Unless injunctive relief is granted, Plaintiffs and California Statewide Class members, who do not have an adequate remedy at law, will continue to suffer harm, and the balance of equities favors Plaintiffs and California Statewide Class members.

221. Plaintiff sand California Statewide Class members seek declaratory and injunctive relief as permitted by law or equity to assure that the Plaintiffs and the California Statewide Class have an effective remedy, including enjoining Equifax from continuing the unlawful practices as set forth above, along with any other relief the Court deems just and proper under the UCL.

222. Plaintiffs also seek reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23 and California Code of Civil Procedure § 1021.5.X.

Claims Asserted on Behalf of the Virginia Statewide Class

COUNT X —
Violation of Virginia Personal Information Breach Notification Act,
Va. Code. §§ 18.2-186.6 et seq.

223. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

224. Plaintiffs Anna Rice-Wright and James R. Wright bring this cause of action on behalf of the Virginia Statewide Class.

225. Virginia law requires that Equifax accurately notify Plaintiffs and Virginia Statewide Class members following discovery or notification of a breach of its data security system (if unencrypted or unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person who will, or it is reasonably believed who will, engage in identify theft or another fraud) without unreasonable delay. Va. Code Ann. § 18.2-186.6(B).

226. Equifax is an entity that owns or licenses computerized data that includes personal information as defined by Va. Code Ann. § 18.2-186.6(B).

227. Plaintiffs and Virginia Statewide Class members' Personal Information (e.g., Social Security numbers) includes personal information as covered under Va. Code Ann. § 18.2-186.6(A).

228. Because Equifax discovered a breach of its security system (in which unencrypted or unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person, who will, or it is reasonably believed who will, engage in identify theft or another fraud), Equifax had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Va. Code Ann. § 18.2-186.6(B).

229. As a direct and proximate result of Equifax's violations of Va. Code Ann. § 18.2-186.6(B), Plaintiffs and Virginia Statewide Class members suffered damages, as described above.

230. Plaintiffs and Virginia Statewide Class members seek relief under Va. Code Ann. § 18.2-186.6(I), including, but not limited to, actual damages.

COUNT XI —
Violation of Virginia Code Annotated § 18.2-186.6

231. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

232. Plaintiffs Anna Rice-Wright and James R. Wright bring this cause of action on behalf of the Virginia Statewide Class.

233. Equifax is an "entity" as defined by section 18.2-186.6(A).

234. Plaintiffs Rice-Wright and Wright and class members are "individuals" as defined by section 18.2-186.6(A).

235. The PII of Plaintiffs and members of the Virginia Statewide Class that was compromised and exposed in the Data Breach constitutes “personal information” as defined by section 18.2-186.6(A), which includes Social Security numbers, driver’s license numbers, financial account numbers, and credit and debit card numbers in combination with security codes, access codes, or passwords that permit access to financial accounts.

236. The breach of the Plaintiffs’ and members of the Virginia Statewide Class’ PII was a “breach of the security system” of Equifax as defined by section 18.2-186.6(A).

237. Under section 18.2-186.6(B), Equifax was required to disclose any breach of the security of its system following discovery or notification of the breach to the Office of the Attorney General and any affected resident of the Commonwealth of Virginia without unreasonable delay.

238. In violation of section 18.2-186.6(B), Equifax unreasonably delayed in-forming Virginia Statewide Class members about the breach of their personal information, and failed to disclose to Virginia Statewide Class members without unreasonable delay that their unencrypted, or not properly and not securely encrypted, personal information had been breached.

239. Upon information and belief, no law enforcement agency instructed Equifax that notification to Virginia Statewide Class members would impede an investigation.

240. As a result of Equifax's violation of section 18.2-186.6, Virginia Statewide Class members have incurred and will incur economic damages to money or property, including but not necessarily limited to: (1) the diminution in the value of their PII; (2) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of financial and medical accounts; (3) lost opportunity costs associated with effort extended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity and health care/medical data misuse; (4) costs associated with the ability to use credit and assets frozen or flagged due to cred-it misuse, including increased costs to use credit, credit scores, credit reports and assets; and (5) tax fraud and/or other unauthorized charges to financial accounts and associated lack of access to funds while proper information is confirmed and corrected..

241. Plaintiffs Rice-Wright and Wright, individually and on behalf of the Virginia Statewide Class, seek all remedies available under section 18.2-186.6,

including but not limited to damages and equitable relief. Plaintiffs also seek reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23 and California Code of Civil Procedure § 1021.5.

Claims Asserted on Behalf of the New Jersey Statewide Class

COUNT XII —
Violation of The New Jersey Consumer Fraud Act
N.J. Stat. Ann. §§ 56:8-1 et seq.

242. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

243. Plaintiff Christopher P. Dunleavy brings this cause of action on behalf of the New Jersey Statewide Class.

244. Equifax, while operating in New Jersey, engaged, in unconscionable commercial practices, deception, misrepresentation, and the knowing concealment, suppression, and omission of material facts with intent that others rely on such concealment, suppression, and omission, in connection with the sale and advertisement of services, in violation of N.J. Stat. Ann. § 56:8-2. This includes, but is not limited to the following:

- Equifax failed to enact adequate privacy and security measures to protect the New Jersey Statewide Class members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

- Equifax failed to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- Equifax knowingly and fraudulently misrepresented that it would maintain adequate data privacy and security practices and procedures to safeguard the New Jersey Statewide Class members' PII from unauthorized dis-closure, release, data breaches, and theft;
- Equifax omitted, suppressed, and concealed the material fact of the inadequacy of its privacy and security protections for the New Jersey Statewide Class members' PII;
- Equifax knowingly and fraudulently misrepresented that it would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the New Jersey Statewide Class members' PII, including but not limited to duties imposed by the FCRA, 15. U.S.C.§ 1681e, and the GLBA, 15 U.S.C. §§ 6801 et seq.;
- Equifax failed to maintain the privacy and security of the New Jersey Statewide Class members' PII, in violation of duties imposed by applicable federal and state laws, including but not limited to those mentioned in the aforementioned paragraph, directly and proximately causing the Data Breach; and
- Equifax failed to disclose the Data Breach to the New Jersey Statewide Class members in a timely and accurate manner, in violation of the duties imposed by N.J. Stat. Ann. § 56:8-163(a).

245. As a direct and proximate result of Equifax's practices, the New Jersey Statewide Class members suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their PII, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their PII.

246. The above unlawful and deceptive acts and practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to the New Jersey Statewide Class members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

247. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard the New Jersey Statewide Class members' PII and that risk of a data breach or theft was highly likely. Equifax's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful.

248. Plaintiffs and the New Jersey Statewide Class members seek relief under N.J. Stat. Ann. § 56:8-19, including, but not limited to, injunctive relief, other equitable actual damages (to be proven at trial), treble damages, and attorneys' fees and costs.

COUNT XIII —
Violation of the New Jersey Customer Security Breach Disclosure Act
N.J. Stat. Ann. §§ 56:8-163 et seq.

249. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

250. Under N.J.S.A. § 56:8-163(b), "[a]ny business ... that compiles or maintains computerized records that include personal information on behalf of another business or public entity shall notify that business or public entity, who shall notify its New Jersey customers ... of any breach of security of the computerized records immediately following discovery, if the personal information was, or is reasonably believed to have been, accessed by an unauthorized person."

251. Equifax is a business that compiles or maintains computerized records that include personal information on behalf of another business under N.J.S.A. § 56:8-163(b).

252. Plaintiffs and the New Jersey Statewide Class members' PII (including but not limited to names, addresses, and social security numbers) includes personal information covered under N.J.S.A. §§ 56:8-163 et seq.

253. Because Equifax discovered a breach of its security system in which personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured, Equifax had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated under N.J.S.A. §§ 56:8-163 et seq.

254. By failing to disclose the Data Breach in a timely and accurate manner, Equifax violated N.J.S.A. § 56:8-163(b).

255. As a direct and proximate result of Equifax's violations of N.J.S.A. § 56:8-163(b), Plaintiffs and the New Jersey Statewide Class members suffered the damages described above.

256. Plaintiffs and the New Jersey Statewide Class members seek relief under N.J.S.A. § 56:8-19, including but not limited to treble damages (to be proven at trial), attorneys' fees and costs, and injunctive relief.

Claims Asserted on Behalf of the Washington Statewide Class

COUNT XIV —
Violation of the Washington Data Brach Notice Act, Wash. Rev. Code. §§ 19.255.10 et seq.

257. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

258. Plaintiffs Victoria Lynn Strutz and Deborah Rivas bring this cause of action on behalf of the Washington Statewide Class.

259. Under Wash. Rev. Code Ann. § 19.255.010(1), "[a]ny person or business that conducts business in this state and that owns or licenses data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person … ."

260. Under Wash. Rev. Code Ann. § 19.255.010(2), "[a]ny person or business that maintains data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

261. Under Wash. Rev. Code Ann. § 19.255.010 (16), "[n]otification to affected consumers … under this section must be made in the most expedient time possible and without unreasonable delay, no more than forty-five calendar days after the breach was discovered."

262. Equifax conducts business in Washington and owns or licenses computerized data that includes personal information, as defined by Wash. Rev. Code Ann. § 19.255.010.

263. Plaintiffs and the Washington Statewide Class members' PII (including but not limited to names, addresses, and social security numbers) includes personal information covered under Wash. Rev. Code Ann. § 19.255.010(5).

264. Because Equifax discovered a breach of its security system in which personal information was, or is reasonably believed to have been, acquired by an

unauthorized person and the personal information was not secured, Equifax had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated under Wash. Rev. Code Ann. § 19.255.010(16).

265. By failing to disclose the Data Breach in a timely and accurate manner, Equifax violated Wash. Rev. Code Ann. § 19.255.010(16).

266. As a direct and proximate result of Equifax's violations of Wash. Rev. Code Ann. § 19.255.010(16), Plaintiffs and the Washington Statewide Class members suffered the damages described above.

267. Plaintiffs and the Washington Statewide Class members seek relief under Wash. Rev. Code Ann. §§ 19.255.010(13)(a), (b) including but not limited to actual damages (to be proven at trial) and injunctive relief.

COUNT XV —
Violation of Washington Consumer Protection Act, Wash. Rev. Code §§ 19.86.020 et seq

268. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

269. Plaintiffs Victoria Lynn Strutz and Deborah Rivas bring this cause of action on behalf of the Washington Statewide Class.

270. Equifax, while operating in Washington, engaged in unfair and deceptive acts and practices in the conduct of trade or commerce, in violation of Wash. Rev. Code § 19.86.020. This includes but is not limited to the following:

- Equifax failed to enact adequate privacy and security measures to protect the Washington Statewide Class members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;
- Equifax failed to take proper action following known security risks, which was a direct and proximate cause of the Data Breach;
- Equifax knowingly and fraudulently misrepresented that it would maintain adequate data privacy and security practices and procedures to safeguard the Washington Statewide Class members' PII from unauthorized disclosure, release, data breaches, and theft;
- Equifax omitted, suppressed, and concealed the material fact of the inadequacy of its privacy and security protections for the Washington Statewide Class members' PII;
- Equifax knowingly and fraudulently misrepresented that it would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the Washington Statewide Class members' PII, including but not limited to duties imposed by the FCRA, 15. U.S.C.§ 1681e, and the GLBA, 15 U.S.C. §§ 6801 et seq.;
- Equifax failed to maintain the privacy and security of the Washington Statewide Class members' PII, in violation of duties imposed by applicable federal and state laws, including but not limited to those mentioned in the aforementioned paragraph, directly and proximately causing the Data Breach; and
- Equifax failed to disclose the Data Breach to the Washington Statewide Class members in a timely and accurate manner, in violation of the duties imposed by Wash. Rev. Code Ann. § 19.255.010(1).

271. As a direct and proximate result of Equifax's practices, the Washington Statewide Class members suffered injury and/or damages, including but not limited to time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their PII.

272. The above unfair and deceptive acts and practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to the Washington Statewide Class members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

273. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard the Washington Statewide Class members' PII and that risk of a data breach or theft was highly likely. Equifax's actions in engaging in the above-described unfair practices and deceptive acts were negligent, knowing and willful.

274. Plaintiffs and the Washington Statewide Class members seek relief pursuant to Wash. Rev. Code § 19.86.090, including but not limited to actual damages (to be proven at trial), treble damages, injunctive relief, and attorneys' fees and costs.

Claims Asserted on Behalf of the District of Columbia Statewide Class

COUNT XVI —
Violation of The District of Columbia Consumer Protection Procedures Act, D.C. Code §§ 28-3904 et seq.

275. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

276. Plaintiff Phillip Williams brings this cause of action on behalf of the District of Columbia Statewide Class.

277. As defined by D.C. Code § 28-3901, D.C. Statewide Class members are "consumers" who did or would have purchased or received consumer goods or services, and who otherwise provide economic demand for Equifax's services.

278. Equifax, while operating in the District of Columbia, used and employed deception, fraud, misrepresentation, and the concealment, suppression, and omission of material facts with intent that others rely upon such concealment, suppression and omission, in connection with the sale and advertisement of services, in violation of D.C. Code § 28-3904. This includes but is not limited the following:

- Equifax failed to enact adequate privacy and security measures to protect the D.C. Statewide Class members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

- Equifax failed to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

- Equifax knowingly and fraudulently misrepresented that it would maintain adequate data privacy and security practices and procedures to safeguard the D.C. Statewide Class members' PII from unauthorized disclosure, release, data breaches, and theft;

- Equifax knowingly omitted, suppressed, and concealed the inadequacy of its privacy and security protections for the D.C. Statewide Class members' PII;

- Equifax knowingly and fraudulently misrepresented that it would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the D.C. Statewide Class members' PII, including but not limited to duties imposed by the FCRA, 15. U.S.C.§ 1681e, and the GLBA, 15 U.S.C. §§ 6801 et seq.;

- Equifax failed to maintain the privacy and security of the D.C. Statewide Class members' PII, in violation of duties imposed by applicable federal and state laws, including but not limited to those mentioned in the aforementioned paragraph, which was a direct and proximate cause of the Data Breach; and

- Equifax failed to disclose the Data Breach to D.C. Statewide Class members in a timely and accurate manner, in violation of D.C. Code § 28-3852(a).

279. As a direct and proximate result of Equifax's practices, the D.C. Statewide Class members suffered the injury and/or damages described herein, including but not limited to time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their PII.

280. The above unfair and deceptive practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to the D.C. Statewide Class members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

281. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard D.C. Statewide Class members' PII and that risk of a data breach or theft was highly likely. Equifax's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the D.C. Statewide Class.

282. Plaintiff and D.C. Statewide Class members seek relief under D.C. Code § 28-3905(k), including, but not limited to, restitution, injunctive relief, punitive damages, attorneys' fees and costs, and treble damages or $1,500 per violation, whichever is greater.

COUNT XVII —
Violation of the District of Columbia Consumer Security Breach Notification Act,
D.C. Code § 28-3851, *et. seq.*

283. Plaintiffs incorporate by reference all paragraphs above as if fully set forth here.

284. Equifax is required to accurately notify Plaintiff and D.C. Statewide Class members if it becomes aware of a breach of their data security system in the most expedient time possible and without unreasonable delay under D.C. Code § 28-3852(a).

285. Equifax owns or licenses computerized data that includes personal information as defined by D.C. Code § 28-3852(a).

286. Plaintiff and D.C. Statewide Class members' PII (including but not limited to names, addresses, and Social Security numbers) includes personal information as covered under D.C. Code § 28-3851(3).

287. Because Equifax was aware of a breach of its security system that was reasonably likely to result in a misuse D.C. residents' personal information, Equifax had an obligation to disclose the Data Breach in a timely and accurate fashion under D.C. Code § 28-3852(a).

288. By failing to disclose the Data Breach in the most expedient time possible and without unreasonable delay, Equifax violated D.C. Code § 28-3852(a).

289. As a direct and proximate result of Equifax's violations of D.C. Code § 28-3852, Plaintiff and the D.C. Statewide Class members suffered the damages alleged herein.

290. Plaintiff and the D.C. Statewide Class members seek relief under D.C. Code § 28-3853(a), including, but not limited to, actual damages and broad equitable relief.

Claims Asserted on Behalf of the Pennsylvania Statewide Class

COUNT XVIII —
Violations of Pennsylvania Unfair Trade Practices And Consumer Protection Law, 73 Pa. Stat. §§ 201-1 et seq.

291. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

292. Plaintiffs Jon M. Lewis, Stephen M. Shafran and Barbara A. Sharfran bring this claim on behalf of the Pennsylvania Statewide Class.

293. Equifax and the Pennsylvania Statewide Class members are “persons” within the meaning of 73 Pa. Stat. Ann. § 201-2.(2).

294. Equifax is engaged in “trade” or “commerce” within the meaning of 73 Pa. Stat. Ann. § 201-2(3).

295. The Pennsylvania Unfair Trade Practices Act (“Pennsylvania UTPA”) prohibits “unfair or deceptive acts or practices in the conduct of any trade or commerce ….” 73 Pa. Stat. Ann. § 201 3.

296. In the course of its business, Equifax, through its agents, employees, and/or subsidiaries, violated the Pennsylvania UTPA as detailed above.

Specifically, Equifax engaged in unlawful, unfair, and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the services purchased by the Pennsylvania Statewide Class in violation of 73 Pa. Cons. Stat. Ann. § 201-3, including but not limited to the following:

- Causing likelihood of confusion or of misunderstanding as to the security of consumer identifying information;
- Failing enact adequate privacy and security measures to protect the Pennsylvania Statewide Class members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;
- Failing to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- Knowingly and fraudulently misrepresented that it would maintain adequate data privacy and security practices and procedures to safeguard the Pennsylvania Statewide Class members' PII from unauthorized disclosure, release, data breaches, and theft;
- Equifax omitted, suppressed, and concealed the material fact of the inadequacy of its privacy and security protections for the Pennsylvania Statewide Class members' PII;
- Engaging in other conduct which created a likelihood of confusion or of misunderstanding; and/or
- Using or employing deception, fraud, false pretense, false promise or misrepresentation, or the concealment, suppression or omission of a material fact with intent that others rely upon such concealment, suppression or omission, in connection with the advertisement and sale of credit furnishing goods and services, whether or not any person has in fact been misled, deceived or damaged thereby.

297. Defendant's concealment of its data security shortcomings was material to Plaintiffs and the Pennsylvania Statewide Class, as Defendant intended. Had they known the truth, Plaintiffs and the Pennsylvania Statewide Class would have taken steps to prevent Equifax from obtaining their personal identifying information.

298. Plaintiffs and Pennsylvania Statewide Class members had no way of discerning that Defendant's representations were false and misleading, or otherwise learning the facts that Defendant had concealed or failed to disclose, because Defendant did not make public that information. Plaintiffs and Pennsylvania Statewide Class members did not, and could not, unravel Defendant's deception on their own.

299. Defendant had an ongoing duty to Plaintiffs and the Pennsylvania Statewide Class to refrain from unfair and deceptive practices under the UTPA in the course of its business. Specifically, Defendant owed Plaintiffs and Pennsylvania Statewide Class members a duty to disclose all the material facts concerning the measures taken to protect class members' sensitive information because it possessed exclusive knowledge, it intentionally concealed it from Plaintiffs and the Pennsylvania Statewide Class, and/or it made misrepresentations that were rendered misleading because they were contradicted by withheld facts.

300. Plaintiffs and Pennsylvania Statewide Class members suffered ascertainable loss and actual damages as a direct and proximate result of Defendant's concealment, misrepresentations, and/or failure to disclose material information.

301. Defendant's violations present a continuing risk to Plaintiffs and the Pennsylvania Statewide Class, as well as to the general public. Defendant's unlawful acts and practices complained of herein affect the public interest.

302. Pursuant to 73 Pa. Stat. Ann. § 201-9.2(a), Plaintiffs and the Pennsylvania Statewide Class seek an order enjoining Defendant's unfair and/or deceptive acts or practices, and awarding damages, punitive and/or treble damages, and any other just and proper relief available under the Pennsylvania UTPA.

Claims Asserted on Behalf of the Delaware Statewide Class

COUNT XIX —
Violation of the Delaware Consumer Fraud Act, 6 Del. Code §§ 2513 et seq.

303. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

304. Plaintiff Gary Martinez brings this cause of action on behalf of the Delaware Statewide Class.

305. Equifax, while operating in Delaware, used and employed deception, fraud, misrepresentation, and the concealment, suppression, and omission of

material facts with intent that others rely upon such concealment, suppression and omission, in connection with the sale and advertisement of services, in violation of 6 Del. Code § 2513(a). This includes but is not limited the following:

- Equifax failed to enact adequate privacy and security measures to protect the Delaware Statewide Class members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;
- Equifax failed to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- Equifax knowingly and fraudulently misrepresented that it would maintain adequate data privacy and security practices and procedures to safeguard the Delaware Statewide Class members' PII from unauthorized disclosure, release, data breaches, and theft;
- Equifax knowingly omitted, suppressed, and concealed the inadequacy of its privacy and security protections for the Delaware Statewide Class members' PII;
- Equifax knowingly and fraudulently misrepresented that it would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the Delaware Statewide Class members' PII, including but not limited to duties imposed by the FCRA, 15. U.S.C.§ 1681e, and the GLBA, 15 U.S.C. §§ 6801 et seq.;
- Equifax failed to maintain the privacy and security of the Delaware Statewide Class members' PII, in violation of duties imposed by applicable federal and state laws, including but not limited to those mentioned in the aforementioned paragraph, which was a direct and proximate cause of the Data Breach; and
- Equifax failed to disclose the Data Breach to the Delaware Statewide Class members in a timely and accurate manner, in violation of 6 Del. Code § 12B-102(a).

306. As a direct and proximate result of Equifax's practices, the Delaware Statewide Class members suffered the injury and/or damages described herein, including but not limited to time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their PII.

307. The above unfair and deceptive practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to the Delaware Statewide Class members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

308. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard the Delaware Statewide Class members' PII and that the risk of a data breach or theft was highly likely. Equifax's actions were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Delaware Statewide Class members.

309. Plaintiff and the Delaware Statewide Class Members seek damages under 6 Del. Code § 2525 for injury resulting from the direct and natural consequences of Defendant's unlawful conduct, in an amount to be proven at trial. *See Stephenson v. Capano Dev., Inc.*, 462 A.2d 1069, 1077 (Del. 1983). Plaintiff

and Delaware Statewide Class members also seek an order enjoining Equifax's unfair, unlawful, and/or deceptive practices, declaratory relief, attorneys' fees (pursuant to 6 Del. Code § 2526), and any other just and proper relief available under the Delaware Consumer Fraud Act, 6 Del. Code §§ 2513 et seq.

COUNT XX —
Violation of the Delaware Computer Security Breach Act, 6 Del. Code §§ 12B-102 et seq.

310. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

311. Plaintiff Gary Martinez brings this cause of action on behalf of the Delaware Statewide Class.

312. Under Del. Code Ann. Tit. 6 § 12b-102(a), "a commercial entity that conducts business in Delaware and that owns or licenses computerized data that includes personal information about a resident of Delaware shall, when it becomes aware of a breach of the security of the system … give notice as soon as possible to the affected Delaware resident. Notice must be made in the most expedient time possible and without unreasonable delay."

313. Under Del. Code Ann. Tit. 6 § 12b-102(b), "a commercial entity that maintains computerized data that includes personal information that the individual or the commercial entity does not own or license shall give notice to and cooperate

with the owner or licensee of the information of any breach of the security of the system immediately following discovery of a breach … .”

314. Equifax is a business that owns or licenses computerized data that includes personal information as defined by 6 Del. Code Ann. §§ 12B-101 et seq.

315. In the alternative, Equifax maintains computerized data that includes personal information that Equifax does not own as defined by 6 Del. Code Ann. §§ 12B-101 et seq.

316. Plaintiff and the Delaware Statewide Class members’ PII (including but not limited to names, addresses, and Social Security numbers) includes personal information covered under 6 Del. Code Ann. § 12B-101(4).

317. Because Equifax was aware of a breach of its security system that was reasonably likely to result in a misuse Delaware residents’ personal information, Equifax had an obligation to disclose the Data Breach in a timely and accurate fashion pursuant to 6 Del. Code Ann. § 12B-102.

318. By failing to disclose the Data Breach in a timely and accurate manner, Equifax violated 6 Del. Code Ann. § 12B-102.

319. As a direct and proximate result of Equifax’s violations of 6 Del. Code Ann. § 12B-102(a), Plaintiff and the Delaware Statewide Class Members suffered the damages alleged herein.

320. Plaintiff and the Delaware Statewide Class members seek relief under 6 Del. Code Ann. § 12B-104, including, but not limited to, actual damages and broad equitable relief.

Claims Asserted on Behalf of the Florida Statewide Class

COUNT XXI —
Violation of Florida's Unfair & Deceptive Trade Practices Act, Fla. Stat. §§ 501.201 et seq.

321. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

322. Plaintiffs Julia A. Williams and Katherine Edwards bring this cause of action on behalf of the Florida Statewide Class.

323. Plaintiffs and the Florida Statewide Class members are "consumers" within the meaning of Fla. Stat. § 501.203(7).

324. Equifax is engaged in "trade" or "commerce" within the meaning of Fla. Stat. § 501.203(8).

325. The Florida Unfair and Deceptive Trade Practices Act ("FUDTPA") makes unlawful "[u]nfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce ..." Fla. Stat. § 501.204(1).

326. In the course of its business, Equifax, through it agents, employees, and/or subsidiaries, violated the FUDTPA as detailed above. Specifically, by failing to take reasonable measures to protect consumer identifying information, failing to promptly notify consumers of the breach of that information, and failing to otherwise adequately prepare for or respond to the breach, Equifax engaged in one or more of the following unfair or deceptive acts or practices prohibited by Fla. Stat. § 501.204(1):

- Failing to maintain adequate and reasonable data security standards to safeguard Florida Statewide Class members' sensitive information from unauthorized disclosure, release, data breaches, and theft, in violation of state and federal laws and its own privacy practices and policies;

- Knowingly and fraudulently misrepresenting that it would maintain adequate and reasonable data security standards for Florida Statewide Class members' sensitive information and safeguard Florida Statewide Class members' sensitive information from unauthorized disclosure, release, data breaches, and theft;

- Knowingly omitting, suppressing, and concealing the inadequacy of its data security protections for the Florida Statewide Class members' sensitive information;

- Failing to disclose the Data Breach to the Florida Statewide Class members in a timely and accurate manner, in violation of Fla. Stat. § 501.171(4); and

327. Defendant's concealment of its data security shortcomings was material to Plaintiffs and the Florida Statewide Class, as Defendant intended. Had

they known the truth, Plaintiffs and the Florida Statewide Class would have taken steps to prevent Equifax from obtaining their personal identifying information.

328. Plaintiffs and Florida Statewide Class members had no way of discerning that Defendant's representations were false and misleading, or otherwise learning the facts that Defendant had concealed or failed to disclose, because Defendant did not make public that information. Plaintiffs and Florida Statewide Class members did not, and could not, unravel Defendant's deception on their own.

329. Defendant had an ongoing duty to Plaintiffs and the Florida Statewide Class to refrain from unfair and deceptive practices under the FUDTPA in the course of its business. Specifically, Defendant owed Plaintiffs and Florida Statewide Class members a duty to disclose all the material facts concerning the measures taken to protect class members' sensitive information because it possessed exclusive knowledge, it intentionally concealed it from Plaintiffs and the Florida Statewide Class, and/or it made misrepresentations that were rendered misleading because they were contradicted by withheld facts.

330. Plaintiffs and Florida Statewide Class members suffered ascertainable loss and actual damages as a direct and proximate result of Defendant's concealment, misrepresentations, and/or failure to disclose material information.

331. Defendant's violations present a continuing risk to Plaintiffs and the Florida Statewide Class, as well as to the general public. Defendant's unlawful acts and practices complained of herein affect the public interest.

332. Pursuant to Fla. Stat. §§ 501.2105(1)-(2), Plaintiffs and the Florida Statewide Class seek an order enjoining Defendant's unfair and/or deceptive acts or practices, and awarding damages and any other just and proper relief available under the FUDTPA.

Claims Asserted on Behalf of the South Carolina Statewide Class

COUNT XXII —
Violation of South Carolina Data Breach Security Act, S.C. Code Ann. §§ 39-1-90 et seq.

333. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

334. Plaintiffs John L. Brisini, Jr., Ryan Treat, Antonietta McCann, Donald A. Cordell, and Patricia Samuelson bring this action on behalf of the South Carolina Statewide Class against Defendant.

335. Equifax is required to accurately notify Plaintiffs and South Carolina Statewide Class members following discovery or notification of a breach of its data security system (if personal information that was not rendered unusable through encryption, redaction, or other methods was, or was reasonably believed to have

been, acquired by an unauthorized person, creating a material risk of harm) in the most expedient time possible and without unreasonable delay under S.C. Code Ann. § 39-1-90(A).

336. Equifax is a business that owns or licenses computerized data or other data that includes personal identifying information as defined by S.C. Code Ann. § 39-1-90(A).

337. Plaintiffs and South Carolina Statewide Class members' Personal Information (e.g., Social Security numbers) includes personal identifying information as covered under S.C. Code Ann. § 39-1-90(D)(3).

338. Because Equifax discovered a breach of its data security system (in which personal information that was not rendered unusable through encryption, redaction, or other methods was, or was reasonably believed to have been, acquired by an unauthorized person, creating a material risk of harm), Equifax had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by S.C. Code Ann. § 39-1-90(A), but failed to do so.

339. As a direct and proximate result of Equifax's violations of S.C. Code Ann. § 39-1-90(A), Plaintiffs and South Carolina Statewide Class members suffered damages, as described above.

340. Plaintiffs and South Carolina Statewide Class members seek relief under S.C. Code Ann. § 39-1-90(G), including, but not limited to, actual damages and injunctive relief.

COUNT XXIII —
Violations of South Carolina Unfair Trade Practices Act, S.C. Code Ann. §§ 39-5-10 et seq.

341. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

342. Plaintiffs John L. Brisini, Jr., Ryan Treat, Antonietta McCann, and Donald A. Cordell, and Patricia Samuelson, Dorchester County, SC bring this action on behalf of the South Carolina Statewide Class against Defendant.

343. Equifax, Plaintiffs, and the South Carolina Statewide Class members are "persons" within the meaning of S.C. Code § 39-5-10(a).

344. Equifax is engaged in "trade" or "commerce" within the meaning of S.C. Code § 39-5-10(b).

345. The South Carolina Unfair Trade Practices Act ("South Carolina UTPA") prohibits "unfair or deceptive acts or practices in the conduct of any trade or commerce." S.C. Code § 39-5-20(a).

346. In the course of its business, Equifax, through its agents, employees, and/or subsidiaries, violated the South Carolina UTPA as detailed above.

Specifically, in failing to adequately protect the sensitive information of South Carolina Statewide Class members and failing to adequately respond to a data breach, Defendant engaged in one or more of the following unfair or deceptive acts or practices in violation of S.C. Code § 39-5-20(a):

- Causing likelihood of confusion or of misunderstanding as to security of South Carolina Statewide Class members' sensitive information;
- Representing that the Equifax's information security systems and practices have characteristics or benefits that they do not have;
- Engaging in other conduct which created a likelihood of confusion or of misunderstanding; and/or
- Using or employing deception, fraud, false pretense, false promise or misrepresentation, or the concealment, suppression or omission of a material fact with intent that others rely upon such concealment, suppression or omission, in connection with the advertisement and sale of Equifax's goods or services, whether or not any person has in fact been misled, deceived or damaged thereby.

347. Defendant's scheme and concealment of the true characteristics of its information security systems were material to Plaintiffs and the South Carolina Statewide Class, as Defendant intended. Had they known the truth, Plaintiffs and the South Carolina Statewide Class would not have permitted Equifax to retain their sensitive information.

348. Plaintiffs and South Carolina Statewide Class members had no way of discerning that Defendant's representations were false and misleading, or

otherwise learning the facts that Defendant had concealed or failed to disclose, because Defendant did not disclose the true nature of its information security systems and practices.

349. Defendant had an ongoing duty to Plaintiffs and the South Carolina Statewide Class to refrain from unfair and deceptive practices under the South Carolina UTPA in the course of its business. Specifically, Defendant owed Plaintiffs and South Carolina Statewide Class members a duty to disclose all the material facts concerning its information security systems and practices because it possessed exclusive knowledge, it intentionally concealed it from Plaintiffs and the South Carolina Statewide Class, and/or it made misrepresentations that were rendered misleading because they were contradicted by withheld facts.

350. Plaintiffs and South Carolina Statewide Class members suffered ascertainable loss and actual damages as a direct and proximate result of Defendant's concealment, misrepresentations, and/or failure to disclose material information.

351. Defendant's violations present a continuing risk to Plaintiffs and the South Carolina Statewide Class, as well as to the general public. Defendant's unlawful acts and practices complained of herein affect the public interest.

352. Pursuant to S.C. Code § 39-5-140(a), Plaintiffs and the South Carolina Statewide Class seek an order enjoining Defendant's unfair and/or deceptive acts or practices, and awarding damages, treble and/or punitive damages, and any other just and proper relief available under the South Carolina UTPA.

Claims Asserted on Behalf of the Louisiana Statewide Class

COUNT XXIV —
Violation of the Louisiana Security Breach Disclosure Act, La. Rev. Stat. §§ 51:3074 et seq.

353. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

354. Plaintiff Randall K. Roshto brings this cause of action on behalf of the Louisiana Statewide Class.

355. Equifax is required to accurately notify Plaintiff and Louisiana Statewide Class members if Equifax becomes aware of a breach of its data security system (that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Louisiana Statewide Class members' Personal Information) in the most expedient time possible and without unreasonable delay under La. Rev. Stat. Ann. § 51:3074(C).

356. Equifax is a business that owns or licenses computerized data that includes personal information as defined by La. Rev. Stat. Ann. § 51:3074(C).

357. Plaintiff's and Louisiana Statewide Class members' Personal Information (e.g., Social Security numbers) includes personal information as covered under La. Rev. Stat. Ann. § 51:3074(C).

358. Because Equifax was aware of a breach of its security system (was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Class members' Personal Information), Equifax had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by La. Rev. Stat. Ann. § 51:3074(C).

359. As a direct and proximate result of Equifax's violations of La. Rev. Stat. Ann. § 51:3074(C), Plaintiff and Louisiana Statewide Class members suffered damages, as described above.

360. Plaintiff and Louisiana Statewide Class members seek relief under La. Rev. Stat. Ann. § 51:3075, including, but not limited to, actual damages.

Claims Asserted on Behalf of the Missouri Statewide Class

COUNT XXV —
Violation of the Missouri Merchandise Practicing Act, Mo. Stat. §§ 407.010 et seq.

361. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

362. Plaintiff Elizabeth Dorssom brings this cause of action on behalf of the Missouri Statewide Class.

363. Equifax, while operating in Missouri, employed deception, misrepresentation, unfair practices, and the concealment, suppression, and omission of material facts in connection with the sale and advertisement of services in violation of Mo. Stat. § 407.020(1). This includes, but is not limited to:

a. Equifax failed to enact adequate privacy and security measures to protect the Missouri Statewide Class members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

b. Equifax failed to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Equifax knowingly and fraudulently misrepresented that it would maintain adequate data privacy and security practices and procedures to safeguard the Missouri Statewide Class members' PII from unauthorized disclosure, release, data breaches, and theft;

d. Equifax omitted, suppressed, and concealed the material fact of the inadequacy of its privacy and security protections for the Missouri Statewide Class members' PII;

e. Equifax knowingly and fraudulently misrepresented that it would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the Missouri Statewide Class members' PII, including but not limited to duties imposed by the FCRA, 15. U.S.C. § 1681e, the GLBA, 15 U.S.C. §§ 6801 et seq., the Missouri Unfair Trade Practice Act, Mo. Stat. § 375.936(4) and (6)(a), and Missouri Statute § 354-525;

f. Equifax failed to maintain the privacy and security of the Missouri Statewide Class members' PII, in violation of duties imposed by applicable federal and state laws, including but not limited to those mentioned in the aforementioned paragraph, directly and proximately causing the Data Breach; and

g. Equifax failed to disclose the Data Breach to the Missouri Statewide Class members in a timely and accurate manner, in violation of the duties imposed by Mo. Rev. Stat. § 407.1500(2)(1)(a).

364. As a direct and proximate result of Equifax's practices, Plaintiff and the Missouri Statewide Class members suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their PII, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their PII.

365. The above unlawful and deceptive acts and practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and the Missouri Statewide Class members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

366. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff's and Missouri Statewide Class members' PII and that risk of a data breach or theft was highly

likely. Equifax's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful.

367. Plaintiff and the Missouri Statewide Class members seek relief under Mo. Ann. Stat. § 407.025, including, but not limited to, injunctive relief, actual damages, punitive damages, and attorneys' fees and costs.

Claims Asserted on Behalf of the Alabama Statewide Class

COUNT XXVI —
Violations of Alabama's Deceptive Trade Practices Act, Code of Ala. §§ 8-19-1 et seq.

368. Plaintiff incorporates by reference all paragraphs above as if fully set forth herein.

369. Plaintiff Karen Bergquist brings this action on behalf of herself and the Alabama Statewide Class against Defendant.

370. Plaintiff is a consumer within the meaning of Code of Ala. § 8-19-3(2).

371. Equifax is engaged in trade and commerce affecting the people of the State of Alabama as defined by Code of Ala. § 8-19-3(8).

372. Plaintiff and Alabama Statewide Class members entrusted Equifax with their PII.

373. As alleged herein, Equifax engaged in unfair or deceptive acts or practices in the conduct of consumer transactions, including the following, in violation of the Alabama Deceptive Trade Practices Act:

- Failure to maintain adequate information security systems and data security practices to safeguard PII belonging to Plaintiff and Alabama Statewide Class members;
- Failure to disclose that its information security systems and data security practices were inadequate to safeguard Plaintiff's and Alabama Statewide Class members' PII from theft;
- Failure to timely and accurately disclose the Data Breach to Plaintiff and Alabama Statewide Class members;
- Representing that Equifax's information security systems and practices have characteristics or benefits that they do not have;
- Causing likelihood of confusion or of misunderstanding as to security of Plaintiff's and Alabama Statewide Class members' sensitive information;
- Engaging in other misleading conduct which created a likelihood of confusion or of misunderstanding;
- Continued acceptance of PII and storage of other personal information after Equifax knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach; and
- Continued acceptance of PII and storage of other personal information after Equifax knew or should have known of the Data Breach and before it allegedly remediated the Breach.

374. As alleged above, Equifax's failure to secure consumers' PII violates the FTCA and therefore violates the Alabama Deceptive Trade Practices Act.

375. Defendant had an ongoing duty to Plaintiff and the Alabama Statewide Class to refrain from misleading and deceptive practices in the course of its business under Alabama Deceptive Trade Practices Act. Specifically, Defendant owed Plaintiff and Alabama Statewide Class members a duty to safeguard Plaintiff's and the Alabama Statewide Class members' sensitive data, to implement state-of-the-art cyber security controls, and to disclose all the material facts concerning its information security systems and practices because Defendant possessed exclusive knowledge, they intentionally concealed it from Plaintiff and the Alabama Statewide Class, and/or they made misrepresentations that were rendered misleading because they were contradicted by withheld facts.

376. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard the PII of Plaintiff and Alabama Statewide Class members, deter hackers, and that the risk of a data breach was highly likely. Furthermore, Defendant knew that, as consumers, Plaintiff and Alabama Statewide Class members would rely upon its deceptive and misleading conduct and could not have discovered the breach on their own.

377. As a direct and proximate result of Equifax's violation of the Alabama Deceptive Trade Practices Act, Plaintiff and Alabama Statewide Class members suffered damages including, but not limited to: an increased cost of credit associated with misuse of their credit data, expenses for credit monitoring and identify theft insurance, other out-of-pocket expenses, anxiety, emotional distress, loss of privacy and other economic and non-economic harm.

378. Defendant's violations present a continuing risk to Plaintiff and the Alabama Statewide Class, as well as to the general public. Defendant's unlawful acts and practices complained of herein affect the public interest.

379. Defendant's unlawful actions have caused and are continuing to cause injury and damages to Plaintiff and Alabama Statewide Class members.

380. On September 28, 2017, a written demand for relief was sent to Equifax complying with Code of Ala. §8-19-10(e). Therefore, Plaintiff and Alabama Statewide Class members seek all damages and relief to which they are entitled.

381. Pursuant to the Code of Ala. §8-19-10(a), Plaintiff and Alabama Statewide Class members are entitled to recover any actual damages, or the sum of $100, whichever is greater as well as, in the Court's discretion, treble damages, costs of litigation and attorney's fees in addition to injunctive relief, including, but

not limited to, enjoining Defendant's unlawful and deceptive acts as set forth above, and such other relief as the Court deems just and proper.

382. Pursuant to Code of Ala. § 8-19-10(a), Plaintiff and Alabama Statewide Class members seek reasonable attorneys' fees and expenses incurred in connection with this action.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of members of the Nationwide Class and Statewide Classes, respectfully request:

383. An order certifying the proposed Class or Classes under the provisions of Rule 23 of the Federal Rules of Civil Procedure, and directing that notice be provided to all members of the Classes;

384. A finding that Equifax breached its duty to safeguard and protect the PII of Plaintiffs and Nationwide Class members that was compromised in the Data Breach;

385. Injunctive relief, including public injunctive relief in the form of an order enjoining Defendant from continuing the unlawful, deceptive, fraudulent, and unfair business practices alleged in this Complaint;

386. That Plaintiffs and Nationwide Class members recover damages in the form of restitution or disgorgement and/or compensatory damages for economic

loss and out-of-pocket costs, treble damages under the applicable federal and state laws, and punitive and exemplary damages under applicable law;

387. A determination that Equifax is financially responsible for all Class notice and administration of Class relief;

388. A judgment against Defendant for any and all applicable statutory and civil penalties;

389. An order requiring Defendant to pay both pre- and post-judgment interest on any amounts awarded;

390. An award to Plaintiffs and Nationwide Class members of costs and reasonable attorneys' fees;

391. Leave to amend this Complaint to conform to the evidence produced in discovery and at trial; and

392. Such other or further relief as the Court may deem appropriate, just, and equitable.

VIII. DEMAND FOR JURY TRIAL

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury of any and all issues in this action so triable.

RESPECTFULLY SUBMITTED this 28th day of September, 2017.

MOTLEY RICE LLC

By: _____*/s/ Kevin R. Dean*___________

Kevin R. Dean (GA Bar #214855)
Jodi Flowers, *pro hac vice forthcoming*
Breanne Cope, *pro hac vice forthcoming*
28 Bridgeside Boulevard
Mount Pleasant, SC 29464
(843) 216-9000, Fax (843) 216-9450
kdean@motleyrice.com
jflowers@motleyrice.com
bcope@motleyrice.com

Laura Ray, *pro hac vice forthcoming*
Mathew Jasinski, *pro hac vice forthcoming*
One Corporate Center
20 Church Street
17th Floor
Hartford, CT 06103
(860) 882-1681, Fax (860) 882-1682
lray@motleyrice.com
mjasinski@motleyrice.com

Lynn Lincoln Sarko, *pro hac vice forthcoming*
Derek W. Loeser, *pro hac vice forthcoming*
Gretchen Freeman Cappio, *pro hac vice forthcoming*
Cari Campen Laufenberg, *pro hac vice forthcoming*
KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101
(206) 623-1900, Fax (206) 623-3384
lsarko@kellerrohrback.com

dloeser@kellerrohrback.com
gcappio@kellerrohrback.com
claufenberg@kellerrohrback.com

Matthew J. Preusch, *pro hac vice forthcoming*
KELLER ROHRBACK L.L.P.
mpreusch@kellerrohrback.com
801 Garden Street, Suite 301
Santa Barbara, CA 93101
(805) 456-1496, Fax (805) 456-1497

Attorneys for Plaintiffs